# The Primitive Soluble Permutation Groups of Degree Less Than 256



Mark William Short

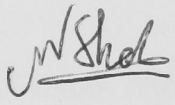
October 1990

A thesis submitted for the degree of Doctor of Philosophy

of The Australian National University

# Declaration

The work in this thesis is my own, except where otherwise stated.



M. W. Short

# Acknowledgements

I am deeply indebted to my supervisors Drs L. G. Kovács and M. F. Newman, who were always willing to set aside time for me. I thank them for all their guidance and inspiration, both that specific to my thesis and that of a more general nature. I also thank my advisor Dr R. A. Bryce for various helpful discussions.

I thank Dr E. A. O'Brien, Werner Nickel and Alice Niemeyer-Nickel for all their constructive comments about aspects of this thesis.

For providing my scholarship I thank the Australian Government and The Australian National University.

Finally, I acknowledge the support of my family and friends. In particular, I am greatly indebted to Hendrik Grundling, Werner Nickel, Alice Niemeyer-Nickel and Eamonn O'Brien for their personal support.

# Abstract

In this thesis we consider the problem of determining all primitive soluble permutation groups of a given degree. A well known theorem of Galois reduces this problem to that of determining the irreducible soluble subgroups of $GL(n,p)$, where $p$ is prime. By attacking the problem in this form, we can make use of the powerful structure theory of Jordan and Suprunenko about irreducible maximal soluble subgroups of general linear groups. In the first part of the thesis we develop this theory a little further. Then we present theorems which together provide a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(2,p)$, and of $GL(q,p)$ for certain primes $q$. We then consider the groups $GL(4,2)$, $GL(4,3)$ and $GL(6,2)$. We find their irreducible soluble subgroups by using a variety of theoretical and computational techniques. The results we obtain allow us to list the primitive soluble permutation groups of degree less than 256. The thesis concludes with a discussion of the provision of access to this list in the form of a CAYLEY library, and of work in progress on extending the list.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Motivation

Permutation groups arose out of the study of roots of polynomials, but soon became objects of independent interest. Early researchers were interested in listing all permutation groups of a given degree. The highest degree for which such a list was made is 11 (Cole (1895), Miller and Ling (1901)). The intransitive groups of a given degree arise (in a suitable sense) from transitive groups of smaller degrees. Consequently, transitive groups received more attention than intransitive ones; lists of all of them were made up to degree 15 (Miller (1897a), Martin (1901), Kuhn (1904)). In a similar way, the transitive groups of a given degree arise from primitive groups of smaller degrees. The primitive groups had only been listed up to degree 20 (Bennett (1912)) until recently, when Sims, with the aid of a computer, prepared a list of all primitive groups up to degree 50. Worthy of special mention is Jordan (1871a), who determined the number of conjugacy classes of primitive maximal soluble permutation groups for all degrees up to one million. A detailed account of the history of listing permutation groups can be found in Appendix A.

The socle of a primitive permutation group is of fundamental importance. This is exploited in the O'Nan-Scott Theorem (see Liebeck, Praeger and Saxl (1988)), in which primitive groups are classified into types according to the structures of their socles and the intersections of these with point stabilisers. Broadly

speaking, primitive groups divide naturally into two types: those with insoluble socle, and those with soluble socle. An extensive list of groups of the first type was given recently by Dixon and Mortimer (1988), who classified all such groups of degree less than 1000.

If a primitive permutation group has soluble socle, then the degree of the group is a prime power, $p^n$ say. Furthermore, the socle is elementary abelian of order $p^n$, and is complemented. The socle may then be treated as an $n$-dimensional vector space over $GF(p)$, and the complement as an irreducible subgroup of $GL(n,p)$. Consequently, the study of primitive permutation groups with soluble socle reduces to the study of irreducible subgroups of $GL(n,p)$. This reduction is essentially due to Galois.

The irreducible subgroups of $GL(n,p)$ also divide naturally into two kinds: those that are insoluble, and those that are soluble. There are many results concerning irreducible insoluble subgroups of $GL(n,p)$, but complete lists of groups of this kind seem to be scarce, especially for $p > 2$. The irreducible insoluble subgroups of $GL(n,2)$ have been listed for all $n \leq 10$ (Kondrat'ev (1986b)). The history of listing linear groups is reviewed briefly in Appendix A.

Irreducible subgroups of $GL(n,p)$ that are soluble are, in general, more numerous than those that are insoluble. The only direct attempt at listing all such groups seems to have been by Harada and Yamaki (1979), who count the irreducible soluble subgroups of $GL(n,2)$ for $n \leq 6$. However, in light of the theorem of Galois mentioned above, Sims' list of primitive permutation groups of degree up to 50 indirectly yields a list of the irreducible soluble subgroups of $GL(n,p)$ for all $p^n \leq 50$. Consequently, and since the subgroups of $GL(1,p)$ are a trivial matter, the irreducible soluble subgroups of $GL(n,p)$ are known for all $p^n < 81$.

This thesis investigates the irreducible soluble subgroups of $GL(n,p)$, or, equivalently, the primitive soluble permutation groups. Although these groups have not featured extensively in lists, there is in fact a very large body of theory about their structure. During the years 1861-1917 this theory was developed almost single-handedly by Jordan, who was inspired by Galois' work on primitive soluble permutation groups and their connection with polynomials soluble by

radicals. This work seems to have attracted very little interest until 1947, when Suprunenko began publishing papers containing not only Jordan's work in more modern notation, but also extensions of it to the case of arbitrary fields. Since that time a number of people have contributed results to this theory.

Irreducible soluble subgroups of $GL(n,p)$ are of considerable interest to those developing soluble quotient algorithms. Such an algorithm takes as input a group given by a finite presentation, and computes special descriptions of the soluble quotients of the group. The nilpotent quotient algorithm (see Newman (1976)) computes such descriptions of the $p$-quotients of a group. This algorithm has proved to be an important tool in the investigation of large Burnside groups. It is expected that an efficient soluble quotient algorithm will be useful in investigating other kinds of large groups.

To indicate the usefulness of having a list of the irreducible soluble subgroups of $GL(n,p)$, we need to give a few more details of a soluble quotient algorithm. We assume by induction that we have a suitable description of a surjective homomorphism $\theta$ from the input group $G$ to a finite soluble group $H$. The aim is then to extend $\theta$, if possible, to a surjective homomorphism $\bar{\theta}$ from $G$ to a downwards extension of $H$ by an elementary abelian $p$-group on which $H$ acts irreducibly. In other words, we try to place an irreducible $GF(p)H$-module under $H$ in such a way that the extended group is also a quotient of $G$. If this step is successful, then we update the description we had of $\theta$ to a description of $\bar{\theta}$. Then the process can be repeated. If we have a list of all the irreducible soluble subgroups of $GL(n,p)$, then we can improve the efficiency of the algorithm in two ways. Firstly, the list could be used to provide a 'head start' for the algorithm—instead of the first step being the search for an abelian quotient of $G$, we could look for homomorphisms from $G$ onto groups on the list. Secondly, instead of computing all the $n$-dimensional irreducible $GF(p)H$-modules, we simply look them up on the list. It is hoped that these modifications to the basic algorithm will lead to a significant gain in efficiency. The idea of looking for homomorphisms from a given group to groups on some list is illustrated in Havas and Kovács (1984), where metacyclic quotients of some knot groups are computed.

The thesis has two main objectives, and both are motivated by the desire to have an efficient soluble quotient algorithm. One of these objectives is to develop algorithms that take as input a positive integer $n$ and a prime $p$, and produce a list of the irreducible soluble subgroups of $GL(n,p)$. The other main objective is to execute these algorithms for those $n$ and $p$ such that $p^n < 256$, and to provide electronic access to the list of groups so obtained. A secondary objective is to 'match', as far as possible, the list of Dixon and Mortimer mentioned above.

## 1.2 Contents of the thesis

As mentioned above, the primitive soluble permutation groups are in one-to-one correspondence with the irreducible soluble linear groups over finite prime fields. In Chapter 2 we exhibit that correspondence in detail, and then proceed to investigate groups of the latter kind. First we summarise the relevant parts of the theory already developed by Jordan and Suprunenko regarding the structure of maximal irreducible soluble linear groups over finite fields. Then we extend that theory as necessary to accomplish the two main objectives stated in the previous section. Table 1.1 shows the primes $p$ and positive integers $n$ for which $p^n < 256$.

| $n$ | $p$ |
|---|---|
| 1 | 2, ..., 251 |
| 2 | 2, ..., 13 |
| 3 | 2, 3, 5 |
| 4 | 2, 3 |
| 5 | 2, 3 |
| 6 | 2 |
| 7 | 2 |

Table 1.1: The values of $p$ and $n$ for which $p^n < 256$

In Chapters 3, 4 and 5 we investigate the irreducible soluble subgroups of $GL(2,\mathbb{F})$, where $\mathbb{F}$ is any finite field. These investigations lead to a list containing exactly one group from each conjugacy class of irreducible soluble subgroups of

$GL(2, \mathbb{F})$.

Chapter 6 presents some results about the maximal irreducible soluble subgroups of $GL(q, \mathbb{F})$, where $q$ is an odd prime. The irreducible soluble subgroups of $GL(3,3)$, $GL(3,5)$ and $GL(5,3)$ are determined.

In Chapter 7 we determine the imprimitive soluble subgroups of $GL(4,2)$ and $GL(4,3)$. We carry out this determination with the help of an algorithm that has been implemented in the group theory system CAYLEY (see below).

In Chapter 8 we develop some 'listing' theorems for the primitive soluble subgroups of $GL(4, \mathbb{F})$ which are similar in nature to those found for $GL(2, \mathbb{F})$.

The algorithm developed in Chapter 7 is used again in Chapter 9, this time to find the irreducible soluble subgroups of $GL(6,2)$.

The final chapter discusses the provision of electronic access to the list of groups. This requires a discussion of CAYLEY, which is a computer system that has extensive capabilities in computing with groups. A full description of this system can be found in Cannon (1984). CAYLEY has a language in which users can write their own programs. An important kind of sub-program is a *procedure*. A procedure is simply a sequence of instructions which one can invoke as part of a larger program. CAYLEY also has a facility called a *library* whereby a user can contribute data and procedures to official releases of the system. All users can then access this information and manipulate it according to their own needs. For example, Sims' list of primitive permutation groups mentioned in the previous section is available as the library PRMGPS. Another example is TWOGPS, a library consisting of the groups of order dividing 128, their automorphism groups, and some procedures for manipulating these groups (see Newman and O'Brien (1989)). I plan to release a CAYLEY library in the near future that will provide access to the primitive soluble permutation groups of degree less than 256. This library is described in Section 10.2. At a later stage the list of groups may also be released as part of the group theory computer system GAP, which is described in Nickel, Niemeyer and Schönert (1988). The final chapter concludes with a note on work in progress on the irreducible soluble subgroups of $GL(8,2)$ (that is, the primitive soluble permutation groups of degree 256).

Appendix A presents a history of the determination of permutation groups and linear groups. Appendix B contains some auxiliary results necessary for the work on $GL(4, \mathbb{F})$ in Chapter 8. Appendix C contains some program listings.

## 1.3 Conventions and Notation

Throughout this thesis all actions are on the right unless specified otherwise. Consequently, if $g$ and $h$ are elements of a group, we define the conjugate $g^h$ of $g$ by $h$ to be $h^{-1}gh$.

If $G$, $N$ and $H$ are groups and $G$ has a normal subgroup isomorphic to $N$ such that $G/N$ is isomorphic to $H$, then we write $G = N \cdot H$. If $G$ has a subgroup isomorphic to $H$ which intersects $N$ trivially, then $G$ is a *semidirect product* of $N$ and $H$, and we write $G = N \rtimes H$.

If $V$ is an $n$-dimensional vector space over the field $\mathbb{F}$, we use the notations $GL(V)$ and $GL(n, \mathbb{F})$ to denote the group of all invertible linear transformations of $V$, or equivalently, the group of all $n$ by $n$ invertible matrices over $\mathbb{F}$. If $\mathbb{F}$ is finite of order $p^k$, we also use the notation $GL(n, p^k)$.

The *dihedral group* $D_{2n}$ of order $2n$ $(n \geq 3)$ is the group

$$\langle a, b \mid a^2 = 1, \quad b^a = b^{-1}, \quad b^n = 1 \rangle .$$

The *generalised quaternion group* $Q_{4n}$ of order $4n$ $(n \geq 2)$ is the group

$$\langle a, b \mid a^2 = b^n, \quad b^a = b^{-1}, \quad b^{2n} = 1 \rangle .$$

The group $Q_8$ is called the *quaternion group.*

The *semidihedral group* $SD_{8n}$ of order $8n$ $(n \geq 2)$ is the group

$$\langle a, b \mid a^2 = 1, \quad b^a = b^{-1+2n}, \quad b^{4n} = 1 \rangle .$$

We denote by $SA_{8n}$ the group of order $8n$ $(n \geq 2)$ given by

$$\langle a, b \mid a^2 = 1, \quad b^a = b^{1+2n}, \quad b^{4n} = 1 \rangle .$$

We say that a group $G$ has a *central decomposition* $(H, K)$ if

1. $H$ and $K$ are normal subgroups of $G$;

2. $G = HK$;

3. $H \cap K \leq Z(H) \cap Z(K)$;

4. $H \cap K$ equals at least one of $Z(H)$ and $Z(K)$.

We also say that $G$ is the *central product* of $H$ and $K$, and write $G = H \Upsilon K$. Note that many authors do not impose the fourth condition.

The *holomorph* of a group $G$, written $\mathrm{Hol}(G)$, is the semidirect product of $G$ and its automorphism group.

We say that a group is *monolithic* if it has a unique minimal normal subgroup.

If $a$, $b$ and $c$ are positive integers such that $a^b$ divides $c$ but that $a^{b+1}$ does not divide $c$, then we say that $a^b$ *sharply divides* $c$, and write $a^b \parallel c$.

We also need some notation for referring to CAYLEY objects. Libraries will be denoted by upper case, for example, PRMGPS. Built-in functions will be denoted by a sans serif font, for example, lattice. Procedures will be denoted by an upper-case typewriter font, for example, GETIRR. Names of algebraic objects, such as sets, will be printed in a lower-case typewriter font, for example, irred.

An index of notation is included at the beginning of the index. Most notation is standard, and can be found, for example, in Robinson (1982).

## 1.4 Polycyclic presentations for finite soluble groups

Finite soluble groups can be uniformly described using polycyclic presentations. Such presentations were introduced by Jürgensen (1970), who used the term AG-system to describe them.

Let $G$ be a finite soluble group. A *polycyclic generating sequence* for $G$ is an ordered set

$$\mathcal{X} := \{a_1 > a_2 > \ldots > a_n\}$$

of elements of $G$ that generates $G$ and such that

$$\langle a_i, \ldots, a_n \rangle \trianglerighteq \langle a_{i+1}, \ldots, a_n \rangle$$

for each $i$. Define $r_i$ by

$$r_i := |\langle a_i, \ldots, a_n \rangle : \langle a_{i+1}, \ldots, a_n \rangle| .$$

A *polycyclic presentation* for $G$ is a presentation $\{\mathcal{X}, \mathcal{R}\}$ in which the relations in $\mathcal{R}$ are of the following two kinds:

1. for $1 \leq i \leq n$ we have the relations

$$a_i^{r_i} = \prod_{k=i+1}^{n} a_k^{\alpha_k},$$

where $0 \leq \alpha_k \leq r_k - 1$;

2. for $1 \leq i < j \leq n$ we have the relations

$$a_j^{a_i} = \prod_{k=i+1}^{n} a_k^{\beta_k},$$

where $0 \leq \beta_k \leq r_k - 1$.

We call this presentation *consistent* if $|G| = r_1 r_2 \ldots r_n$. If $\{\mathcal{X}, \mathcal{R}\}$ is consistent, then every element $g$ of $G$ can be written uniquely in the form

$$g = \prod_{i=1}^{n} a_i^{\varepsilon_i},$$

where $0 \leq \varepsilon_i \leq r_i - 1$. The *normal form* of $g$ (with respect to $\mathcal{X}$) refers to either the word $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \ldots a_n^{\varepsilon_n}$ or the sequence $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$.

All soluble groups discussed in detail in this thesis will be described using consistent polycyclic presentations.

# Chapter 2

# Background theory

The main results in this chapter are of two kinds: one kind deals with the structure of primitive maximal soluble permutation groups in general, and the other kind deals with the construction, up to permutational isomorphism, of the primitive maximal soluble permutation groups of certain degrees.

## 2.1 Primitive soluble permutation groups

In this section we use without definition the concepts of primitive and imprimitive permutation groups, systems of imprimitivity and their refinements, and the wreath product of permutation groups. These are all basic concepts and are discussed in many books on group theory, for example, Robinson (1982).

**2.1.1 Notation.** We use $\mathrm{Sym}(X)$ to mean the symmetric group on the set $X$, and $S_n$ to mean the symmetric group on the set of the first $n$ positive integers. If $G$ and $H$ are permutation groups, we denote the wreath product of $G$ and $H$ by $G \operatorname{wr} H$, where $G$ is a co-ordinate subgroup and $H$ is the top group.

**2.1.2 Definition.** Let $G$ and $H$ be permutation groups acting on the sets $X$ and $Y$, respectively. We say that $G$ and $H$ are *permutationally isomorphic* if there exist a bijection $\beta : X \to Y$ and an isomorphism $\mu : G \to H$ such that $(xg)\beta = (x\beta)(g\mu)$ for all $x \in X$ and for all $g \in G$. We call the pair $(\beta, \mu)$ a *permutational isomorphism* from $G$ to $H$.

Note that two permutation groups acting on the same set are permutationally isomorphic if and only if they are conjugate in the symmetric group on that set. We say that a permutation group of degree $n$ is *maximal soluble* if it is permutationally isomorphic to a maximal soluble subgroup of $S_n$.

Although we are only interested in primitive soluble permutation groups, it is necessary (as will become clear in Theorem 2.5.4) to know something about imprimitive soluble permutation groups.

**2.1.3 Theorem.** *Let $n$ be a positive integer, let $M$ be a transitive but imprimitive maximal soluble subgroup of $S_n$, and let*

$$\Gamma := \{X_1, \ldots, X_m\}$$

*be an unrefinable system of imprimitivity for $M$. Let $\theta : M \to \mathrm{Sym}(\Gamma)$ be the homomorphism defined by*

$$\forall g \in M \quad X_i(g\theta) := X_i g\,.$$

*Then $\mathbf{N}_M(X_1)|_{X_1}$ is a primitive maximal soluble subgroup of $\mathrm{Sym}(X_1)$, $M\theta$ is a transitive maximal soluble subgroup of $\mathrm{Sym}(\Gamma)$, and $M$ is permutationally isomorphic to $\mathbf{N}_M(X_1)|_{X_1}$ wr $M\theta$.*

**Proof.** The primitivity of $\mathbf{N}_M(X_1)|_{X_1}$ follows from the unrefinability of $\Gamma$, and the transitivity of $M\theta$ follows from the transitivity of $M$. Let $P$ be any subgroup of $\mathrm{Sym}(X_1)$ containing $\mathbf{N}_M(X_1)|_{X_1}$, and let $T$ be any subgroup of $\mathrm{Sym}(\Gamma)$ containing $M\theta$. A method for proving that $M$ is permutationally isomorphic to a subgroup of $P \,\mathrm{wr}\, T$ is given in the proof of Theorem II.1.2 of Huppert (1967, p. 145) (although the result stated there is weaker), and so we will not give a proof of that fact. Now suppose that $P$ and $T$ are chosen as above but with the extra condition that they be maximal soluble. Then $P \,\mathrm{wr}\, T$ is soluble, and so by the maximality of $M$, we must have that $M = P \,\mathrm{wr}\, T$. It then follows that $\mathbf{N}_M(X_1)|_{X_1} = P$ and $M\theta = T$. ∎

**2.1.4 Theorem.** *Let $n$ be a positive integer, let $M$ and $\bar{M}$ be transitive but imprimitive maximal soluble subgroups of $S_n$, and let*

$$\Gamma := \{X_1, \ldots, X_m\} \quad \textit{and} \quad \bar{\Gamma} := \{\bar{X}_1, \ldots, \bar{X}_{\bar{m}}\}$$

*be unrefinable systems of imprimitivity for* $M$ *and* $\bar{M}$. *Let* $\theta : M \to \mathrm{Sym}(\Gamma)$ *and* $\bar{\theta} : \bar{M} \to \mathrm{Sym}(\bar{\Gamma})$ *be the homomorphisms defined by*

$$\forall g \in M \quad X_i(g\theta) := X_i g \quad \text{and} \quad \forall \bar{g} \in \bar{M} \quad \bar{X}_i(\bar{g}\bar{\theta}) := \bar{X}_i \bar{g}\,.$$

*Then* $M$ *and* $\bar{M}$ *are conjugate if and only if*

1. $m = \bar{m}$;
2. $\mathbf{N}_M(X_1)|_{X_1}$ *is permutationally isomorphic to* $\mathbf{N}_{\bar{M}}(\bar{X}_1)|_{\bar{X}_1}$, *and;*
3. $M\theta$ *is permutationally isomorphic to* $\bar{M}\bar{\theta}$.

**Proof.** Suppose that $M$ is conjugate to $\bar{M}$, say $M^\pi = \bar{M}$ for some $\pi \in S_n$. Then

$$\Gamma\pi := \{X_1\pi, \ldots, X_m\pi\}$$

is another system of imprimitivity for $\bar{M}$. We will show that $\Gamma\pi = \bar{\Gamma}$. Suppose that $\Gamma\pi \neq \bar{\Gamma}$. Then it is easy to see that $\bar{M}$ preserves the set of all non-empty $X_i\pi \cap \bar{X}_j$, as $i$ runs from 1 to $m$ and $j$ runs from 1 to $\bar{m}$. Obviously this set is a refinement of $\bar{\Gamma}$, and so, by the unrefinability of $\bar{\Gamma}$, it either equals $\bar{\Gamma}$, or each non-empty $X_i\pi \cap \bar{X}_j$ is a singleton. By our assumption, the latter must be the case. If $X_i\pi \cap \bar{X}_j$ is not empty, denote its unique element by $x_{ij}$. It is clear that there exist $i$, $j$ and $k$ such that the elements $x_{i1}$, $x_{j1}$ and $x_{ik}$ are pairwise distinct. By the previous theorem, $\bar{M}$ contains an element $\bar{g}$ (in $\mathbf{N}_{\bar{M}}(\bar{X}_1)|_{\bar{X}_1}$) satisfying

$$x_{i1}\bar{g} = x_{j1} \quad \text{and} \quad x_{ik}\bar{g} = x_{ik}\,.$$

The first of these properties implies that $X_i\pi\bar{g} = X_j\pi$ and yet the second property implies that $X_i\pi\bar{g} = X_i\pi$, contradicting the fact that $\Gamma\pi$ is preserved by $\bar{M}$. Therefore $\Gamma\pi = \Gamma$. It is then clear that $m = \bar{m}$, that the pair

$$\beta : X_i \mapsto X_i\pi \quad \text{and} \quad \mu : g \mapsto g^\pi$$

defines a permutational isomorphism from $M\theta$ to $\bar{M}\bar{\theta}$, and that the pair

$$\gamma : x \mapsto xt\pi \quad \text{and} \quad \nu : g \mapsto g^{t\pi}$$

defines a permutational isomorphism from $\mathbf{N}_M(X_1)|_{X_1}$ to $\mathbf{N}_{\bar{M}}(\bar{X}_1)|_{\bar{X}_1}$, where $t$ is an element of $M$ such that $X_1t\pi = \bar{X}_1$.

The proof in the other direction is straight-forward and so we omit it. ■

The significance of the previous two theorems is that each imprimitive maximal soluble permutation group $M$ has a canonical wreath decomposition $P \operatorname{wr} T$, where $P$ and $T$ have smaller degree than $M$, and where $P$ is primitive maximal soluble and $T$ is transitive maximal soluble. In other words, $M$ is an iterated wreath product of primitive maximal soluble permutation groups of smaller degrees. Note that the maximality assumption is critical in the proofs of these theorems. So now, if we know all primitive maximal soluble permutation groups of degree less than some bound, and if we can decide which of their iterated wreath products of degree less than that bound are maximal soluble, then in fact we know all transitive maximal soluble permutation groups of degree less than that bound. It is clear from Jordan's enumerations of transitive maximal soluble permutation groups (see Appendix A) that Jordan 'knew' the previous two theorems, although I do not know of any formal proofs of them in his work. A brief description of the results is contained, for example, in Jordan (1917), where it is claimed (p. 269) that the only time that an iterated wreath product of the above kind is not maximal soluble is when two consecutive wreath factors have degree 2.

Now we are ready to study primitive soluble permutation groups. Our first theorem shows that we only need to consider degrees which are a power of a prime; Huppert (1967, Theorem II.3.2, p. 159) attributes this result to Galois.

**2.1.5 Theorem.** *Every primitive soluble permutation group has prime power degree.* ■

The following reduction theorem is well known and very important for our purposes. Huppert (1967, Theorem II.3.2, p. 159) attributes part (d) to Galois.

**2.1.6 Theorem.** *Let $p$ be a prime, let $n$ be a positive integer and let $V$ be the vector space of dimension $n$ over the field of $p$ elements. If $G$ is a subgroup of $GL(V)$, denote by $V \rtimes G$ the permutation group of degree $p^n$ that is the semidirect product of $V$ (acting on itself by translation) and $G$ (acting in the natural way) considered as a subgroup of* $\mathrm{Sym}(V)$. *Let $\mathcal{S}$ be a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(V)$.*

*(a) If $G \in \mathcal{S}$, then $V \rtimes G$ is a primitive soluble permutation group of degree $p^n$.*

*(b) If $G \in \mathcal{S}$, and $H$ is a subgroup of $GL(V)$ that is conjugate to $G$, then $V \rtimes H$ is conjugate in* $\mathrm{Sym}(V)$ *to $V \rtimes G$.*

*(c) If $G \in \mathcal{S}$, and $H$ is a subgroup of $GL(V)$ that is not conjugate to $G$, then $V \rtimes H$ is not conjugate to $V \rtimes G$.*

*(d) If $P$ is a primitive soluble subgroup of* $\mathrm{Sym}(V)$*, then there is a group $G$ in $\mathcal{S}$ such that $V \rtimes G$ is conjugate to $P$.* ■

This theorem shows that the problem of finding a complete and irredundant set of conjugacy class representatives the primitive soluble subgroups of $S_{p^n}$ is equivalent to that of finding a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(n,p)$. By viewing the original problem in this second form we can make great progress by exploiting the substantial body of theory developed by Jordan and Suprunenko on maximal irreducible soluble subgroups of general linear groups. We will take up this approach later on in this chapter (Section 2.5), but first we need some results from other parts of group theory.

**2.1.7 Remark.** The above theorem is sufficient to give the primitive soluble subgroups of $S_p$ ($p$ prime), because $GL(1,p)$ is cyclic of order $p-1$. Clearly there is exactly one conjugacy class of primitive soluble subgroups of $S_p$ for each divisor of $p-1$. Jordan (1867) wrote that this was known to Galois, and that Galois also predicted that there would be a single conjugacy class of primitive maximal soluble subgroups of $S_{p^n}$ for any $n$; Jordan showed this not to be the case, even for $n = 2$.

## 2.2 Some results from representation theory

In this section we present some miscellaneous results that we need from representation theory.

**2.2.1 Theorem.** *Let $\mathbb{F}$ be a field, let $G$ be a finite group, let $n$ be a positive integer, and suppose that there exist faithful irreducible $\mathbb{F}$-representations of $G$ of dimension $n$. For such a representation $\rho$, denote by $[\rho]$ the class of all $\mathbb{F}$-representations of $G$ that are equivalent to $\rho$, and denote by $L$ the group $GL(n, \mathbb{F})$. Recall that $\mathrm{Aut}(G)$ has a natural left-action on the set of all $[\rho]$ given by $\alpha([\rho]) := [\alpha\rho]$, where $\alpha$ is an automorphism of $G$, and $g(\alpha\rho) := (g\alpha)\rho$ for all $g \in G$. Then we have the following results:*

*(a)* $\mathbf{N}_L(G\rho)/\mathbf{C}_L(G\rho)$ *is isomorphic to* $\mathbf{C}_{\mathrm{Aut}(G)}([\rho])$*;*

*(b) the index of* $\mathbf{C}_{\mathrm{Aut}(G)}([\rho])$ *in* $\mathrm{Aut}(G)$ *is equal to the length of the orbit containing* $[\rho]$*;*

*(c) the number of orbits under this action is equal to the number of conjugacy classes of subgroups of $L$ that are irreducible and isomorphic to $G$.*

**Proof.** Part (a) is easy to prove, and parts (b) and (c) follow from the Orbit-Stabiliser Theorem. ■

The tensor product of matrices is a well known construction: the reason we give it below is to establish the order we will use on the basis vectors of the tensor product of the underlying spaces.

**2.2.2 Definition.** Let $a$ be an $m$ by $n$ matrix over a ring and let $b$ be an $r$ by $s$ matrix over the same ring. We define the *tensor product*, $a \otimes b$, of these matrices to be the $mr$ by $ns$ matrix whose $(i, j)$-th $m$ by $n$ block is $b_{ij}a$.

**2.2.3 Proposition.** *Let $a$ and $b$ be square matrices over the same ring, and let $k$ be an integer. Then $(a \otimes b)^k = a^k \otimes b^k$.* ■

## 2.3 Irreducible cyclic groups over finite fields

The results in this section (except possibly the last proposition) seem to be part of the folklore.

**2.3.1 Notation.** Let $p$ be a prime, let $k$ and $n$ be positive integers, and let $\mathbb{F}$ be the field of $p^k$ elements.

**2.3.2 Theorem.** *There exists an irreducible cyclic subgroup of order $m$ in $GL(n, \mathbb{F})$ if and only if $m$ divides $p^{kn} - 1$ and $m$ does not divide $p^{kd} - 1$ for any positive integer $d < m$.* ■

**2.3.3 Theorem.** *If there exist irreducible cyclic subgroups of order $m$ in $GL(n, \mathbb{F})$, then they lie in a single conjugacy class.* ■

**2.3.4 Definition.** In $GL(n, \mathbb{F})$ the irreducible cyclic subgroups of order $p^{kn} - 1$ are called the *Singer cycles.*

**2.3.5 Theorem.** (see Huppert (1967, Theorem II.7.3a, p. 187)) *Let $G$ be an irreducible subgroup of a Singer cycle $S$ of $GL(n, \mathbb{F})$. Then the centraliser in $GL(n, \mathbb{F})$ of $G$ is $S$, and the normaliser in $GL(n, \mathbb{F})$ of $G$ is the semidirect product of $S$ and a cyclic group $C$ of order $n$. The action of one generator of $C$ on $G$ is $p^k$-th powering.* ■

We now give a method of constructing the normaliser of a Singer cycle. Let $x^n + \lambda_{n-1}x^{n-1} + \ldots + \lambda_0$ be a polynomial over $\mathbb{F}$ with splitting field $\mathbb{E}$, and such that one of its roots has multiplicative order $p^{kn} - 1$ in $\mathbb{E}$ (a so-called *primitive* polynomial). Consider $\mathbb{E}$ as a vector space over $\mathbb{F}$ with basis $\{1, x, x^2, \ldots, x^{n-1}\}$, and let $z$ be the matrix of the linear map $v \mapsto vx$, that is, $z$ is the matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\lambda_0 & -\lambda_1 & -\lambda_2 & \cdots & -\lambda_{n-1} \end{pmatrix}.$$

Then $z$ generates a Singer cycle of $GL(n, \mathbb{F})$. Let $a$ be the matrix of the linear map $v \mapsto v^{p^k}$ (which generates the Galois group of $\mathbb{E}$ over $\mathbb{F}$). Therefore, the $i$-th row of $a$ is the first row of $z^{(i-1)p^k}$. Then $a$ has order $n$, $a^{-1}za = z^{p^k}$, and $\{a, z\}$ generates the normaliser of the Singer cycle $\langle z \rangle$.

In the case when $n = 2$, there is an explicit form for the matrix $a$ above.

**2.3.6 Proposition.** *Let $x^2 + \mu x + \lambda$ be a primitive polynomial over $\mathbb{F}$, and set*

$$a := \begin{pmatrix} 1 & 0 \\ -\mu & -1 \end{pmatrix} \quad \text{and} \quad z := \begin{pmatrix} 0 & 1 \\ -\lambda & -\mu \end{pmatrix}.$$

*Then $a$ and $z$ correspond to their namesakes in the above construction.*

**Proof.** All we need to check is that the second row of $a$ equals the first row of $z^{p^k}$. Let $\xi$ be a root of the polynomial in the statement of the proposition; then $\xi^{p^k}$ is the other root. Therefore $\xi + \xi^{p^k} = -\mu$ and so, by the Cayley-Hamilton Theorem, $z + z^{p^k} = -\mu I_2$, where $I_2$ denotes the identity matrix. The result then follows. ■

## 2.4 Extraspecial $q$-groups

Throughout this section $q$ is a prime. A detailed analysis of the irreducible soluble subgroups of $GL(n, p)$ (see next section) requires intimate knowledge of certain aspects of the representation theory of extraspecial $q$-groups, and of certain groups associated with them. In this section we present various theorems about such groups.

**2.4.1 Definition.** An *extraspecial $q$-group* is a finite non-abelian $q$-group whose centre, derived group and Frattini subgroup coincide and have order $q$.

**2.4.2 Theorem.** (see Suzuki (1986, 4.13, p. 67)) *There are exactly two isomorphism types of non-abelian groups of order $q^3$, and both are extraspecial. If $q$ is odd, then one has exponent $q$ and the other has exponent $q^2$. If $q = 2$, then both have exponent 4; one is the dihedral group $D_8$ and the other is the quaternion group $Q_8$.* ■

**2.4.3 Theorem.** (see Suzuki (1986, Theorem 4.18, p. 69)) *Let $G$ be an extraspecial $q$-group. Then $G$ has order $q^{1+2l}$ for some positive integer $l$ and exactly one of the following holds:*

*(a) $q$ is odd, $G$ has exponent $q$, and is the central product of $l$ non-abelian groups of order $q^3$ and exponent $q$;*

*(b) $q$ is odd, $G$ has exponent $q^2$, and is the central product of $l-1$ non-abelian groups of order $q^3$ and exponent $q$ and one non-abelian group of order $q^3$ and exponent $q^2$;*

*(c) $q=2$, and $G$ is the central product of $l$ copies of $D_8$;*

*(d) $q=2$, and $G$ is the central product of $l-1$ copies of $D_8$ and one $Q_8$.* ■

The central decompositions above are not unique (for example $D_8 \Upsilon D_8$ is isomorphic to $Q_8 \Upsilon Q_8$), but they are the ones that we will use throughout this thesis.

The Fitting subgroup of a primitive soluble linear group over a finite field has the property that each of its abelian characteristic subgroups is cyclic (see Corollary 2.5.9). It is the next structure theorem of P. Hall that makes extraspecial $q$-groups so important for us.

**2.4.4 Theorem.** (see Suzuki (1986, Theorem 4.22, p. 75)) *Let $G$ be a finite $q$-group in which every abelian characteristic subgroup is cyclic. Then exactly one of the following holds:*

*(a) $q$ is odd, and $G$ is either cyclic, or the central product of a cyclic group and an extraspecial $q$-group of exponent $q$;*

*(b) $q=2$, and $G$ is cyclic, dihedral, semidihedral, generalised quaternion, or the central product of any one of the four kinds of groups just mentioned and an extraspecial 2-group.* ■

The following is a useful corollary. The proof is routine and will be omitted.

**2.4.5 Corollary.** *Let $G$ be a finite $q$-group in which every abelian characteristic subgroup is cyclic and central. Then $G$ is either cyclic, or the central product of a cyclic group and an extraspecial $q$-group. If $q$ is odd, the extraspecial group has exponent $q$. If $q=2$, then $G \ncong D_8$.* ■

Now we investigate the automorphism groups of extraspecial $q$-groups.

**2.4.6 Theorem.** *(a)* (see Winter (1972)) *Let $G$ be an extraspecial $q$-group of order $q^{1+2l}$ and exponent $q$ or 4. The group of automorphisms of $G$ that act trivially on both $Z(G)$ and $G/Z(G)$ is equal to* $\mathrm{Inn}(G)$. *Let $H$ be the normal subgroup of* $\mathrm{Aut}(G)$ *consisting of those elements that act trivially on $Z(G)$. Then $H/\mathrm{Inn}(G)$ is isomorphic to a subgroup of the symplectic group $Sp(2l,q)$. If $q$ is odd, then $H/\mathrm{Inn}(G)$ is isomorphic to the full symplectic group $Sp(2l,q)$. If $G$ is the central product of $l$ copies of $D_8$, then $H/\mathrm{Inn}(G)$ is isomorphic to the orthogonal group $O^+(2l,2)$. If $G$ is the central product of $l-1$ copies of $D_8$ and one $Q_8$, then $H/\mathrm{Inn}(G)$ is isomorphic to the orthogonal group $O^-(2l,2)$.*
*(b) Let $G$ be the central product of a cyclic group of order 4 and an extraspecial 2-group. The group of automorphisms of $G$ that act trivially on both $Z(G)$ and $G/Z(G)$ is equal to* $\mathrm{Inn}(G)$. *If $H$ is the normal subgroup of* $\mathrm{Aut}(G)$ *consisting of those elements that act trivially on $Z(G)$, then $H/\mathrm{Inn}(G)$ is isomorphic to the symplectic group $Sp(2l,2)$.* ■

The above theorem actually occurs in a disguised form in Bolt, Room and Wall (1961-62, Corollary 3 on p. 66, Theorem 4 on p. 67, lines 9-10 on p. 83, Theorem 5 on p. 84, Theorem 5* on p. 87). It is also shown there that if $q$ is odd, then $H$ splits over $\mathrm{Inn}(G)$, and it is remarked that if $q = 2$, $H$ does not in general split over $\mathrm{Inn}(G)$.

A brief explanation of why symplectic groups are involved in the automorphism groups of extraspecial $q$-groups is that commutation in $G$ defines a symplectic form on the $GF(q)$-vector space $G/G'$. Every element of $H$ must preserve this symplectic form, and hence $H/\mathrm{Inn}(G)$ can be viewed as a subgroup of $Sp(2l,q)$. When $q = 2$, a quadratic form is also involved. Here the group $O^+(2l,2)$ is the group of all linear transformations that preserve the quadratic form

$$f(x_1,\ldots,x_{2l}) = x_1x_2 + \ldots + x_{2l-1}x_{2l}\ ,$$

and the group $O^-(2l,2)$ is the group of all linear transformations that preserve the quadratic form

$$f(x_1,\ldots,x_{2l}) = x_1x_2 + \ldots + x_{2l-1}x_{2l} + x_{2l-1}^2 + x_{2l}^2.$$

The following theorem seems to be part of the folklore.

**2.4.7 Theorem.** *(a) Let $G$ be an extraspecial $q$-group of order $q^{1+2l}$, and let $\mathbb{E}$ be a finite field in which there are primitive $q$-th roots of unity. Then $\mathbb{E}$ is a splitting field for $G$, and $G$ has exactly $q-1$ equivalence classes of faithful (absolutely) irreducible representations over $\mathbb{E}$, each of degree $q^l$. These representations are distinguished from one another by their restrictions to $Z(G)$. Furthermore, the equivalence classes of these representations are permuted transitively by the automorphism group of $G$ and hence there is a unique conjugacy class of irreducible subgroups of $GL(q^l, \mathbb{E})$ that are isomorphic to $G$.*
*(b) Let $G$ be the central product of a cyclic group of order 4 and an extraspecial 2-group of order $2^{1+2l}$, and let $\mathbb{E}$ be a finite field containing a primitive 4-th root of unity. Then $G$ has exactly two faithful (absolutely) irreducible representations over $\mathbb{E}$, each of degree $2^l$. These representations are distinguished from each other by their restrictions to $Z(G)$. There is an automorphism of $G$ that interchanges the equivalence classes of these two representations, and therefore there is a unique conjugacy class of irreducible subgroups of $GL(2^l, \mathbb{E})$ that are isomorphic to $G$.* ■

We are now in a position to obtain the results that will be of direct use to us when we investigate the structure of irreducible soluble linear groups in the next section.

**2.4.8 Notation.** Let $\mathbb{E}$ be a finite field containing primitive $q$-th roots of unity. In $GL(q^l, \mathbb{E})$ let $G$ be an (absolutely) irreducible extraspecial $q$-subgroup of order $q^{1+2l}$ and exponent $q$ or 4, and let $F$ be the group generated by $G$ and the scalar group (that is, $F = G\mathbf{C}_{GL(q^l,\mathbb{E})}(G)$).

Abstractly speaking, $F$ is a central product of $G$ and a cyclic group of order $|\mathbb{E}| - 1$. If $q$ is odd, then there is just one choice, up to isomorphism, for $G$, but if $q = 2$, then there are two possible isomorphism types for $G$. Under certain conditions, however, the isomorphism type of $F$ is independent of the isomorphism type of $G$: the following result is well known.

**2.4.9 Proposition.** *If $C$ is a cyclic group containing elements of order 4, then $C \curlyvee Q_8$ is isomorphic to $C \curlyvee D_8$.* ■

This result, together with Theorem 2.4.3, shows that if $q = 2$ and $\mathbb{E}$ has primitive 4th roots of unity, then there is just one possible isomorphism type for $F$, even though there are two for $G$.

**2.4.10 Notation.** If $q$ is odd, we say $F$ has *type I.* If $q = 2$ and $\mathbb{E}$ has 4th roots of unity, we say $F$ has *type II.* If $q = 2$ and $\mathbb{E}$ does not have 4th roots of unity, we say $F$ has *type III.* If $F$ has type III and $G$ is $D_8 \curlyvee \ldots \curlyvee D_8$, we say $F$ has *type III(a).* If $F$ has type III and $G$ is $D_8 \curlyvee \ldots \curlyvee D_8 \curlyvee Q_8$, we say $F$ has *type III(b).*

If $F$ has type I or III, then the subgroup generated by the elements of order $q$ or 4, respectively, is just $G$, and so $G$ is characteristic in $F$. If $F$ has type II, then the (characteristic) subgroup generated by the elements of order 4 is $C_4 \curlyvee G$.

It is necessary for us to have a canonical set of matrices which generates $F$. We choose a set which exhibits the central decomposition of $G$ as described in Theorem 2.4.3. The generators of $G$ come in pairs $(u_i, v_i)$, with each pair generating an extraspecial $q$-group of order $q^3$, and members of distinct pairs commuting. More explicitly,

$u_i^q = v_i^q = I_{q^l}$, except when $F$ has type III(b); in this case the last pair of generators satisfies instead $u_l^2 = v_l^2 = -I_{q^l}$;

$[u_j, u_i] = I_{q^l}$ ;

$[v_j, v_i] = I_{q^l}$ ;

$$[v_j, u_i] = \begin{cases} I_{q^l} & \text{if } j \neq i, \\ \varepsilon I_{q^l} & \text{if } j = i, \end{cases}$$

where $\varepsilon$ is a primitive $q$-th root of unity in $\mathbb{E}$. Note that these relations, together with the obvious relations that involve a generator for the scalar group, yield a polycyclic presentation for $F$. The following method of constructing matrices

$u_i$ and $v_j$ satisfying the above relations was apparently known to Jordan (see Dieudonné (1961, p. xxxviii)). Let $u$ and $v$ be the $q$ by $q$ matrices defined by

$$u := \begin{pmatrix} 0 & 1 \\ I_{q-1} & 0 \end{pmatrix} \quad \text{and} \quad v := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \varepsilon & 0 & \cdots & 0 \\ 0 & 0 & \varepsilon^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \varepsilon^{q-1} \end{pmatrix}.$$

Note that $[v, u] = \varepsilon I_q$. For $1 \leq i \leq l$ define $u_i$ and $v_i$ by

$$u_i := I_{q^{l-i}} \otimes u \otimes I_{q^{i-1}} \quad \text{and} \quad v_i := I_{q^{l-i}} \otimes v \otimes I_{q^{i-1}} \ ;$$

however, if $F$ has type III(b), we define $u_l$ and $v_l$ instead by

$$u_l := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes I_{q^{l-1}} \quad \text{and} \quad v_l := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} \otimes I_{q^{l-1}},$$

where $\alpha$ and $\beta$ are two fixed elements from the prime subfield of $\mathbb{E}$ such that $\alpha^2 + \beta^2 = -1$.

Now we seek a method of identifying and constructing the normaliser in $GL(q^l, \mathbb{E})$ of $F$. This normaliser is perhaps the most important group in the whole theory concerned with the structure of irreducible soluble linear groups.

**2.4.11 Notation.** Denote by $N$ the normaliser in $GL(q^l, \mathbb{E})$ of $F$.

**2.4.12 Theorem.**

$$N/F \cong \begin{cases} Sp(2l, q) & \textit{if } F \textit{ has type I or II}, \\ O^+(2l, 2) & \textit{if } F \textit{ has type III(a)}, \\ O^-(2l, 2) & \textit{if } F \textit{ has type III(b)}. \end{cases}$$

**Proof.** Since $F$ is absolutely irreducible, its centraliser in $GL(q^l, \mathbb{E})$ is the scalar group (its centre). Let $\rho$ be the defining representation of $F$. If $F$ has type I or III, then from Theorem 2.2.1 we have that

$$\begin{aligned} N/Z(F) &\cong \{\theta \in \mathrm{Aut}(F) \mid \theta\rho \text{ is equivalent to } \rho\} \\ &\cong \{\theta \in \mathrm{Aut}(G) \mid \theta\rho \text{ is equivalent to } \rho\} \\ &= \{\theta \in \mathrm{Aut}(G) \mid (\theta\rho)|_{Z(G)} \text{ is equivalent to } \rho|_{Z(G)}\} \\ &= H. \end{aligned}$$

If $F$ has type II, we have from the same theorem that

$$\begin{aligned} N/Z(F) &\cong \{\theta \in \mathrm{Aut}(F) \mid \theta\rho \text{ is equivalent to } \rho\} \\ &\cong \{\theta \in \mathrm{Aut}(C_4 \curlyvee G) \mid \theta\rho \text{ is equivalent to } \rho\} \\ &= \{\theta \in \mathrm{Aut}(C_4 \curlyvee G) \mid (\theta\rho)|_{Z(G)} \text{ is equivalent to } \rho|_{Z(G)}\} \\ &= H. \ \blacksquare \end{aligned}$$

The above result is not new—Jordan apparently knew it in the cases when $F$ has type I or III (see Dieudonné (1961)), while Suprunenko (1976, Theorem 20.16, p. 151) proves it when $F$ has type I or II. It also occurs in full in Bolt, Room and Wall (1961-62, Theorem 5 on p. 67, Theorem 5 on p. 84, Theorem 5* on p. 87), although the theorem and proof are given in the context of the complex field. However, the above proof seems to be new.

**2.4.13 Theorem.** *The centraliser in $GL(q^l, \mathbb{E})$ of $F/Z(F)$ is $F$.*

**Proof.** This follows from Theorem 2.4.6. ■

Note that the above proof is much simpler than that given by Suprunenko (1976, Theorem 20.4, p. 142).

Having identified the normaliser of $F$, we now discuss a way to construct it. As already mentioned, $N$ is very important; it is unfortunate that the theorems dealing with its construction are aesthetically unpleasant. However, the reader should not be deceived by this, for neither the statements of the theorems nor their proofs are as complicated as they may first appear.

The notation in the following theorems is cumulative; that is, later theorems in this section use notation established in earlier theorems.

**2.4.14 Theorem.** *Define the map $\theta : N \to GL(2l, q)$ by*

$$g\theta := \begin{pmatrix} \alpha_{11} & \beta_{11} & \dots & \alpha_{1l} & \beta_{1l} \\ \gamma_{11} & \delta_{11} & \dots & \gamma_{1l} & \delta_{1l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{l1} & \beta_{l1} & \dots & \alpha_{ll} & \beta_{ll} \\ \gamma_{l1} & \delta_{l1} & \dots & \gamma_{ll} & \delta_{ll} \end{pmatrix},$$

*where*

$$u_i^g = \lambda_i u_1^{\alpha_{i1}} v_1^{\beta_{i1}} \dots u_l^{\alpha_{il}} v_l^{\beta_{il}},$$
$$v_i^g = \mu_i u_1^{\gamma_{i1}} v_1^{\delta_{i1}} \dots u_l^{\gamma_{il}} v_l^{\delta_{il}},$$

*for some scalars $\lambda_i$ and $\mu_i$. Then $\theta$ is a homomorphism with kernel $F$.*

**Proof.** It is routine (but tedious) to check that $\theta$ is a homomorphism. The assertion that $\theta$ has kernel $F$ follows from the previous theorem. ■

**2.4.15 Theorem.** *Let $\Phi$ be the $2l$ by $2l$ block diagonal matrix with the matrix*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

*running down its diagonal. If $F$ has type I or II, then define $S$ by*

$$S := \{x \in GL(2l, q) \mid x\Phi x^T = \Phi\}.$$

*Then the image of $\theta$ is $S$ (and therefore $S \cong Sp(2l, q)$.)*

The following proof occurs in Suprunenko (1976, Lemma 20.7, p. 150), but it contains some ideas which are important for us and so we repeat it.

**Proof.** Since $g \in N$ acts like an automorphism of $F$, the $u_i^g$ and $v_j^g$ must satisfy the same relations as the $u_i$ and $v_j$. Therefore,

$$(u_i^g)^q = (v_i^g)^q = I_{q^l},$$
$$\left[u_j^g, u_i^g\right] = I_{q^l},$$
$$\left[v_j^g, v_i^g\right] = I_{q^l},$$
$$\left[v_j^g, u_i^g\right] = \begin{cases} I_{q^l} & \text{if } i \neq j, \\ \varepsilon I_{q^l} & \text{if } i = j. \end{cases}$$

Since $F' \leq Z(F)$, it is not difficult to derive the following relations:

$[u_j^g, u_i^g]$ is $\varepsilon$ raised to the power of

$$\sum_{k=1}^{l} (\alpha_{ik}\beta_{jk} - \alpha_{jk}\beta_{ik});$$

$[v_j^g, v_i^g]$ is $\varepsilon$ raised to the power of

$$\sum_{k=1}^{l} (\gamma_{ik}\delta_{jk} - \gamma_{jk}\delta_{ik});$$

$[v_j^g, u_i^g]$ is $\varepsilon$ raised to the power of

$$\sum_{k=1}^{l}(\alpha_{ik}\delta_{jk} - \beta_{ik}\gamma_{jk}) .$$

Therefore,

$$\begin{aligned}
\textstyle\sum_{k=1}^{l}(\alpha_{ik}\beta_{jk} - \alpha_{jk}\beta_{ik}) &\equiv 0 \bmod q \ , \\
\textstyle\sum_{k=1}^{l}(\gamma_{ik}\delta_{jk} - \gamma_{jk}\delta_{ik}) &\equiv 0 \bmod q \ , \\
\textstyle\sum_{k=1}^{l}(\alpha_{ik}\delta_{jk} - \beta_{ik}\gamma_{jk}) &\equiv \begin{cases} 0 \bmod q & \text{if } i \neq j, \\ 1 \bmod q & \text{if } i = j. \end{cases}
\end{aligned}$$

It then follows that $(g\theta)\Phi(g\theta)^T = \Phi$. To prove the surjectivity of $\theta$, take an element of $S$, say

$$\begin{pmatrix}
\alpha_{11} & \beta_{11} & \dots & \alpha_{1l} & \beta_{1l} \\
\gamma_{11} & \delta_{11} & \dots & \gamma_{1l} & \delta_{1l} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\alpha_{l1} & \beta_{l1} & \dots & \alpha_{ll} & \beta_{ll} \\
\gamma_{l1} & \delta_{l1} & \dots & \gamma_{ll} & \delta_{ll}
\end{pmatrix} .$$

Let $z$ be a generator for the scalar group of $GL(q^l, \mathbb{E})$. Consider the maps $\xi : F \to F$, defined by

$$\begin{aligned}
u_i^\xi &:= \lambda_i u_1^{\alpha_{i1}} v_1^{\beta_{i1}} \dots u_l^{\alpha_{il}} v_l^{\beta_{il}} , \\
v_i^\xi &:= \mu_i u_1^{\gamma_{i1}} v_1^{\delta_{i1}} \dots u_l^{\gamma_{il}} v_l^{\delta_{il}} , \\
z^\xi &:= z ,
\end{aligned}$$

where the $\lambda_i$ and $\mu_i$ are scalars. If any such map were an automorphism of $F$, then it would be realised in $N$, because $N/Z(F)$ is isomorphic to the group of all automorphisms of $F$ that act trivially on $Z(F)$. This would then establish the surjectivity of $\theta$. If $F$ has type I, we set all the $\lambda_i$ and $\mu_i$ to be 1. If $F$ has type II, we choose the $\lambda_i$ and $\mu_i$ according to the following rules:

$$\begin{aligned}
\lambda_i^2 &= \begin{cases} 1 & \text{if } \sum_{k=1}^{l} \alpha_{ik}\beta_{ik} \equiv 0 \bmod 2, \\ -1 & \text{otherwise;} \end{cases} \\
\mu_i^2 &= \begin{cases} 1 & \text{if } \sum_{k=1}^{l} \gamma_{ik}\delta_{ik} \equiv 0 \bmod 2, \\ -1 & \text{otherwise.} \end{cases}
\end{aligned}$$

It is then routine to check that $\xi$ is a homomorphism. Since $F$ is nilpotent, $\xi$ is faithful if and only if it is faithful on $Z(F)$ (see Theorem 3.2.5). But this happens by construction, and so $\xi$ is an automorphism of $F$. ■

Note that it is not necessary to prove the surjectivity of $\theta$ in such an explicit way, since the definition given for $S$ is well known to be a definition of $Sp(2l,q)$, and we already know that $\ker\theta = F$ and that $N/F \cong Sp(2l,q)$.

**2.4.16 Theorem.** *If $F$ has type III(a), then define $S$ by*

$$\begin{aligned} S \;:=\; \{x \in GL(2l,q) \mid\; & x\Phi x^T = \Phi, \\ & x_{i1}x_{i2} + \ldots + x_{i,2l-1}x_{i,2l} = 0, \quad 1 \le i \le 2l\}. \end{aligned}$$

*Then the image of $\theta$ is $S$ (and therefore $S \cong O^+(2l,2)$.)*

**Proof.** By the same reasoning as in the previous proof, $(g\theta)\Phi(g\theta)^T = \Phi$. The relations

$$u_i^2 = v_i^2 = I_{2l}$$

lead to the equations

$$\begin{aligned} \textstyle\sum_{k=1}^{l} \alpha_{ik}\beta_{ik} &\equiv 0 \bmod 2, \\ \textstyle\sum_{k=1}^{l} \gamma_{ik}\delta_{ik} &\equiv 0 \bmod 2. \end{aligned}$$

Therefore the image of $\theta$ is a subgroup of (the set) $S$. By following the surjectivity argument in the previous proof, we choose an element from $S$, set the $\lambda_i$ and $\mu_i$ to be 1, and the result follows. ■

**2.4.17 Theorem.** *If $F$ has type III(b), then define $S$ by the set of all elements $x$ of $GL(2l,q)$ such that $x\Phi x^T = \Phi$ and*

$$x_{i1}x_{i2} + \ldots + x_{i,2l-1}x_{i,2l} + x_{i,2l-1} + x_{i,2l} = \begin{cases} 0, & 1 \le i \le 2l-2, \\ 1, & 2l-1 \le i \le 2l. \end{cases}$$

*Then the image of $\theta$ is $S$ (and therefore $S \cong O^-(2l,2)$.)*

**Proof.** By similar reasoning as in the previous proof, $(g\theta)\Phi(g\theta)^T = \Phi$. We also have the relations

$$u_i^2 = v_i^2 = \begin{cases} I_{2l} & \text{if } i \ne l, \\ \varepsilon I_{2l} & \text{if } i = l. \end{cases}$$

These lead to the equations

$$\sum_{k=1}^{l} \alpha_{ik}\beta_{ik} + \alpha_{il} + \beta_{il} \equiv \begin{cases} 0 \bmod 2 & \text{if } i \neq l, \\ 1 \bmod 2 & \text{if } i = l, \end{cases}$$

$$\sum_{k=1}^{l} \gamma_{ik}\delta_{ik} + \gamma_{il} + \delta_{il} \equiv \begin{cases} 0 \bmod 2 & \text{if } i \neq l, \\ 1 \bmod 2 & \text{if } i = l. \end{cases}$$

Therefore the image of $\theta$ is a subgroup of (the set) $S$. By following the argument in the previous proof, we choose an element from $S$, set the $\lambda_i$ and $\mu_i$ to be 1, and the result follows. ■

As far as I am aware, the last two theorems are new, although Jordan may have known them. Note that their proofs give somewhat oblique proofs of the isomorphism type of $S$ (it is not clear to me how the definition of $S$ even implies that $S$ is a group); there may be direct proofs of this in the literature, but I have not been able to find one.

**2.4.18 Notation.** There are usually many copies of $Sp(2l, q)$ in $GL(2l, q)$. From now on in this thesis, whenever we talk about $Sp(2l, q)$, $O^+(2l, 2)$ and $O^-(2l, 2)$, we will always mean the groups defined in the statements of the previous three theorems.

To construct a generating set for $N$, we actually need a generating set for $S$ and an inverse of $\theta$. We find an inverse image of a matrix from $S$ by viewing it the manner suggested by Thereom 2.4.14, and then constructing an inverse image $g \in GL(q^l, \mathbb{E})$ by finding a solution to the system of $2lq^{2l}$ linear equations in $q^{2l} + 2l$ unknowns produced by knowing the action that $g$ has on the $u_i$ and $v_j$. So if we have a generating set for $S$, then we can find matrices which, together with $F$, generate $N$. Obviously, as $l$ grows this task involves exponentially increasing amounts of linear algebra.

## 2.5 The irreducible soluble subgroups of $GL(n, p)$

In this section we give the important theoretical results on which the thesis depends. Much of this theory was developed by Jordan in the years 1861-1917 and

Suprunenko in the years 1947-1972. Exactly how much of the theory should be attributed to Jordan is unclear to me. He wrote over 600 pages on the topic, and had certainly discovered some powerful structure theorems about linear groups over finite fields. Whether his proofs are correct is another matter—I found that trying to decipher his work was not a worthwhile expenditure of time. Of great assistance, however, is a summary of Jordan's work in this area written by Dieudonné (1961). If Dieudonné's reading of Jordan is correct, then Suprunenko follows Jordan very closely, but applies the theory to linear groups over arbitrary fields. Although Suprunenko says little about Jordan in his two books (1963 and 1976) on this subject (I cannot speak for his papers), one gets the feeling that he had read Jordan reasonably carefully, because he even uses the same notation, sometimes in places where it would have been more natural[1] to use something else in Russian. For example, both use the symbol $F$ to denote a certain abelian normal subgroup of a linear group (the group we will denote by $A$); presumably Jordan uses this symbol because it is the first letter of the word *faisceau*, a term he uses to mean 'subgroup'. In any case, Suprunenko's treatment is more general than Jordan's and, as far as I can tell, correct.

Although we are only interested in irreducible soluble linear groups over finite prime fields, it is necessary (and no extra work) to develop the theory over arbitrary finite fields.

**2.5.1 Notation.** Let $p$ be a prime, let $k$ and $n$ be positive integers and let $\mathbb{F}$ be the field of $p^k$ elements.

The strategy we use is to investigate the structures of the irreducible maximal soluble subgroups of $GL(n, \mathbb{F})$. Later chapters deal with the determination of their irreducible subgroups for restricted values of $n$ and $p^k$. The structure of an irreducible maximal soluble subgroup of $GL(n, \mathbb{F})$ depends very much on whether the group is (linearly) primitive or imprimitive:

**2.5.2 Definition.** Let $G$ be an irreducible subgroup of $GL(n, \mathbb{F})$, acting on the

[1] According to L. G. Kovács

vector space $V$. We call $G$ *imprimitive* if there exists a decomposition

$$V = V_1 \oplus \ldots \oplus V_r \quad (r > 1)$$

of $V$ that is preserved under the action of $G$. We call the set $\{V_1, \ldots, V_r\}$ a *system of imprimitivity* for $G$, and each member of this set is called a *block of imprimitivity* for $G$. The minimum of the set of dimensions of the blocks of imprimitivity for $G$ is called the *minimal block size* of $G$. If $G$ is not imprimitive, we call $G$ *primitive*.

We already have used the words 'primitive' and 'imprimitive' in the context of permutation groups, but this duplication is standard and should cause no confusion.

Note that in the above definition the irreducibility of $G$ implies that $G$ acts transitively on each system of imprimitivity. Therefore the number $r$ above is a divisor of $n$.

**2.5.3 Notation.** Let $m$ be a proper divisor of $n$, let $P$ be an irreducible subgroup of $GL(m, \mathbb{F})$, and let $T$ be a transitive subgroup of $S_{n/m}$. We now construct a subgroup of $GL(n, \mathbb{F})$ called the *wreath product* of $P$ and $T$, and denoted by $P \operatorname{wr} T$. Let $\{\bar{g}_1, \ldots, \bar{g}_r\}$ be a generating set for $P$, and let $\{\sigma_1, \ldots, \sigma_s\}$ be a generating set for $T$. For each generator $\bar{g}_i$ of $P$, take the matrix $I_{n/m}$, and replace the (1,1) entry by $\bar{g}_i$, the other diagonal entries by $I_m$, and the off-diagonal entries by the $m$ by $m$ zero matrix. Call this $n$ by $n$ matrix $g_i$. Convert each generator $\sigma_i$ of $T$ to an $n/m$ by $n/m$ permutation matrix $\bar{t}_i$ in the usual way, and set $t_i := I_m \otimes \bar{t}_i$. Then $P \operatorname{wr} T$ is the group generated by the $g_i$ and $t_i$.

It is well known (see, for example, Suprunenko (1976, Lemma 15.4, p. 107)) that the group $P \operatorname{wr} T$ above is irreducible except when $P$ is the trivial group (in which case $m = 1$, as $P$ is irreducible). Note that these (irreducible) wreath products are obviously imprimitive. In fact, every imprimitive subgroup of $GL(n, \mathbb{F})$ is conjugate to a subgroup of some wreath product like that above. Compare the following theorem with Theorem 2.1.3.

**2.5.4 Theorem.** (see Suprunenko (1976, Theorem 15.4, p. 109)) *Let $M$ be an imprimitive maximal soluble subgroup of $GL(n, \mathbb{F})$, and let*

$$\Gamma := \{V_1, \ldots, V_m\}$$

*be an unrefinable system of imprimitivity for $M$. Let $\theta : M \to \mathrm{Sym}(\Gamma)$ be the homomorphism defined by*

$$\forall g \in M \quad V_i(g\theta) := V_i g\,.$$

*Then $\mathbf{N}_M(V_1)\,|_{V_1}$ is a primitive maximal soluble subgroup of $GL(V_1)$, $M\theta$ is a transitive maximal soluble subgroup of $\mathrm{Sym}(\Gamma)$, and $M$ is linearly isomorphic to $\mathbf{N}_M(V_1)|_{V_1}$ wr $M\theta$.* ■

**2.5.5 Remark.** Consider the case when $m = n$ in the above theorem. Then $V_1$ is 1-dimensional, and so $\mathbf{N}_M(V_1)|_{V_1} = GL(1, \mathbb{F})$. By hypothesis, $M$ is irreducible, and therefore we must have $p^k > 2$ (see the paragraph before the previous theorem). In particular, $GL(n, 2)$ contains no imprimitive subgroups if $n$ is prime.

The proof of the following theorem is entirely similar to that of Theorem 2.1.4 and so we omit it.

**2.5.6 Theorem.** *Let $M$ and $\bar{M}$ be imprimitive maximal soluble subgroups of $GL(n, \mathbb{F})$, and let*

$$\Gamma := \{V_1, \ldots, V_m\} \quad \textit{and} \quad \bar{\Gamma} := \{\bar{V}_1, \ldots, \bar{V}_{\bar{m}}\}$$

*be unrefinable systems of imprimitivity for $M$ and $\bar{M}$. Let $\theta : M \to \mathrm{Sym}(\Gamma)$ and $\bar{\theta} : \bar{M} \to \mathrm{Sym}(\bar{\Gamma})$ be the homomorphisms defined by*

$$\forall g \in M \quad V_i(g\theta) := V_i g \quad \textit{and} \quad \forall \bar{g} \in \bar{M} \quad \bar{V}_i(\bar{g}\bar{\theta}) := \bar{V}_i \bar{g}\,.$$

*Then $M$ and $\bar{M}$ are conjugate if and only if*

1. *$m = \bar{m}$;*
2. *$\mathbf{N}_M(V_1)|_{V_1}$ is linearly isomorphic to $\mathbf{N}_{\bar{M}}(\bar{V}_1)|_{\bar{V}_1}$, and;*
3. *$M\theta$ is permutationally isomorphic to $\bar{M}\bar{\theta}$.* ■

We now give a construction theorem for the imprimitive maximal soluble subgroups of $GL(n, \mathbb{F})$. The proof is routine and so we omit it.

**2.5.7 Theorem.** *Let $m$ be a proper divisor of $n$, let $\mathcal{P}_m$ be a complete and irredundant set of conjugacy class representatives of the primitive maximal soluble subgroups of $GL(m, \mathbb{F})$, and let $\mathcal{T}_{n/m}$ be a complete and irredundant set of conjugacy class representatives of the transitive maximal soluble subgroups of $S_{n/m}$. Define the set $\mathcal{S}_m$ of imprimitive soluble subgroups of $GL(n, \mathbb{F})$ by*

$$\mathcal{S}_m := \{P \operatorname{wr} T \mid P \in \mathcal{P}_m\,,\ T \in \mathcal{T}_{n/m}\}\,.$$

*However, if $p^k = 2$, then define the set $\mathcal{S}_1$ to be empty (see Remark 2.5.5). Let $\mathcal{S}$ be the union of the $\mathcal{S}_m$ as $m$ runs through the proper divisors of $n$. Then those members of $\mathcal{S}$ that are maximal soluble form a complete and irredundant set of conjugacy class representatives of the imprimitive maximal soluble subgroups of $GL(n, \mathbb{F})$.* ■

The previous three theorems show that if we know for each proper divisor $m$ of $n$ the primitive maximal soluble subgroups of $GL(m, \mathbb{F})$ and the transitive maximal soluble subgroups of $S_{n/m}$, and if we can decide which of their wreath products of the above kind are maximal soluble, then we can construct a complete and irredundant set of conjugacy class representatives of the imprimitive maximal soluble subgroups of $GL(n, \mathbb{F})$. Therefore we need no further theory to deal with these subgroups of $GL(n, \mathbb{F})$, other than finding a method of deciding which of the $P \operatorname{wr} T$ above are maximal soluble. Whether such a wreath product is maximal soluble seems to be highly dependent upon $n$ and $p^k$, and so we do not attempt a general treatment of this problem.

The rest of this section deals with the primitive maximal soluble subgroups of $GL(n, \mathbb{F})$. To begin with, we develop the theory in full generality, but later we introduce some restrictions.

**2.5.8 Theorem.** (see Suprunenko (1976, Lemma 19.1, p. 129)) *If $G$ is a primitive subgroup of $GL(n, \mathbb{F})$, then every abelian normal subgroup of $G$ is cyclic.* ■

**2.5.9 Corollary.** *If $G$ is a primitive subgroup of $GL(n, \mathbb{F})$, and $N$ is a nilpotent normal subgroup of $G$, then every abelian characteristic subgroup of $N$ is cyclic. Therefore the structure of $O_q(N)$ is given by Theorem 2.4.4.* ■

**2.5.10 Notation.** Set $L := GL(n, \mathbb{F})$, and let $M$ be a primitive maximal soluble subgroup of $L$.

In what follows, the reader may find Figure 2.1 helpful.

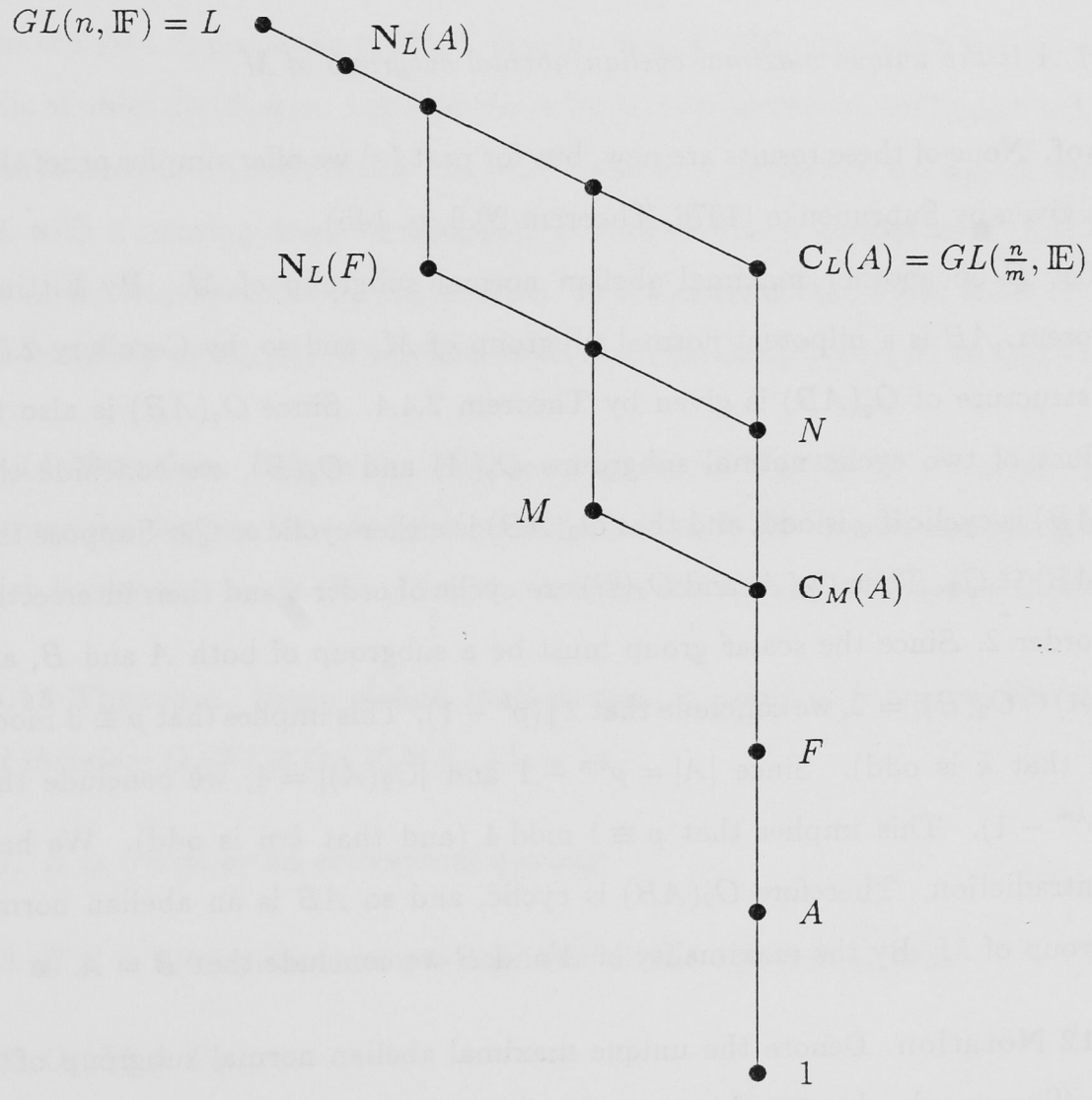



Figure 2.1: Some important subgroups of $L$ related to $M$

**2.5.11 Theorem.** (see Suprunenko (1976, Lemma 19.1, p. 129, Theorem 20.9, p. 145)) *Let $A$ be a maximal abelian normal subgroup of $M$. Then the following statements hold:*

*(a) A is conjugate to a group of block diagonal matrices, where each block is the same, and is m by m say, where m is a divisor of n;*

*(b) the linear span, $\mathbb{E}$, of the powers of any one of the m by m diagonal blocks of A is an extension field of $\mathbb{F}I_m$;*

*(c) the degree of this field extension is m;*

*(d) A is isomorphic to the multiplicative group of $\mathbb{E}$: in particular, A is cyclic of order $p^{km} - 1$;*

*(e) A is the unique maximal abelian normal subgroup of M.*

**Proof.** None of these results are new, but for part (e) we offer simpler proof than that given by Suprunenko (1976, Theorem 20.9, p. 145).

Let $B$ be another maximal abelian normal subgroup of $M$. By Fitting's Theorem, $AB$ is a nilpotent normal subgroup of $M$, and so, by Corollary 2.5.9, the structure of $O_q(AB)$ is given by Theorem 2.4.4. Since $O_q(AB)$ is also the product of two cyclic normal subgroups $O_q(A)$ and $O_q(B)$, we conclude that $O_q(AB)$ is cyclic if $q$ is odd, and that $O_2(AB)$ is either cyclic or $Q_8$. Suppose that $O_2(AB) \cong Q_8$. Then $O_2(A)$ and $O_2(B)$ are cyclic of order 4 and their intersection has order 2. Since the scalar group must be a subgroup of both $A$ and $B$, and $|O_2(A) \cap O_2(B)| = 2$, we conclude that $2 \| (p^k - 1)$. This implies that $p \equiv 3 \bmod 4$ (and that $k$ is odd). Since $|A| = p^{km} - 1$ and $|O_2(A)| = 4$, we conclude that $4 \| (p^{km} - 1)$. This implies that $p \equiv 1 \bmod 4$ (and that $km$ is odd). We have a contradiction. Therefore $O_2(AB)$ is cyclic, and so $AB$ is an abelian normal subgroup of $M$. By the maximality of $A$ and $B$ we conclude that $B = A$. ∎

**2.5.12 Notation.** Denote the unique maximal abelian normal subgroup of $M$ by $A$ (Suprunenko denotes this group by $F$), and let $m$ be the divisor of $n$ such that $A$ has order $p^{km} - 1$. Let $\bar{z}$ be a fixed generator of a fixed Singer cycle of $GL(m, \mathbb{F})$, obtained by the method described in Section 2.3, and let $\mathbb{E}$ be the field of $p^{km}$ elements that is the linear span of the powers of $\bar{z}$. Let $z$ be the block scalar matrix of $GL(n, \mathbb{F})$ with $\bar{z}$ running down its diagonal. It is clear from the above theorem and Theorem 2.3.3 that $A$ is conjugate to the group generated

by $z$. Without loss of generality, we replace $M$ by a suitable conjugate so that $A = \langle z \rangle$.

**2.5.13 Theorem.** $\mathbf{C}_L(A) = GL(n/m, \mathbb{E})$. *Furthermore,* $\mathbf{C}_L(A)$ *is complemented in* $\mathbf{N}_L(A)$ *by a cyclic group of order* $m$*; in particular,* $M/\mathbf{C}_M(A)$ *is cyclic of order dividing* $m$*. The action of one generator of the complement to is to* $p^k$*-th power each* $m$ *by* $m$ *block of* $\mathbf{C}_L(A)$.

**Proof.** The proof of the first statement is routine and so we omit it. Also, it is known (see Suprunenko (1976, Theorem 20.1, p. 138)) that $\mathbf{N}_L(A)/\mathbf{C}_L(A)$ is cyclic of order dividing $m$. Let $\bar{a}$ be the $m$ by $m$ matrix constructed by the method given in Section 2.3 such that $\bar{a}^{-1}\bar{z}\bar{a} = \bar{z}^{p^k}$, and let $a$ be the block diagonal matrix of $L$ with $\bar{a}$ running down its diagonal. It is clear that $a$ normalises $\mathbf{C}_L(A)$ and acts in the way specified in the theorem. It is also clear that $a$ has order $m$ and acts faithfully on $\mathbf{C}_L(A)$. Therefore $\langle a \rangle$ is a complement in $\mathbf{N}_L(A)$ to $\mathbf{C}_L(A)$. ∎

**2.5.14 Notation.** Denote the Fitting subgroup of $\mathbf{C}_M(A)$ by $F$. (Note that Suprunenko denotes $\mathbf{C}_M(A)$ by $V$ and in place of $F$ he chooses another group, which he denotes by $A$: this $A$ turns out to be the Fitting subgroup of $\mathbf{C}_M(A)$.)

**2.5.15 Theorem.** *Every abelian characteristic subgroup of* $F$ *is contained in* $A$*, and therefore* $O_q(F) \cong O_q(A)$ Y $E$*, where*

1. $E$ *is trivial or an extraspecial* $q$*-group;*

2. *if* $E$ *is extraspecial and* $q$ *is odd, then* $E$ *has exponent* $q$*, and;*

3. $O_2(F) \ncong D_8$.

**Proof.** Since $A \trianglelefteq M$, it follows that $\mathbf{C}_M(A) \trianglelefteq M$, and therefore $F \trianglelefteq M$. The maximality of $A$ gives us that $Z(F) = A$. The uniqueness of $A$ then implies that every abelian characteristic subgroup of $F$ is a subgroup of $A$. In particular, every abelian characteristic subgroup of $O_q(F)$ is a subgroup of $O_q(A)$, and so the result follows from Corollary 2.4.5. ∎

The reader should keep in mind that $\mathbb{E}$ is a field of $m$ by $m$ matrices, and that $A$ is the scalar group of $GL(n/m, \mathbb{E})$. It makes sense, then, to ask whether subgroups of $GL(n/m, \mathbb{E})$ are irreducible when viewed as consisting $n/m$ rows and columns of elements from $\mathbb{E}$. In particular, such a group is absolutely irreducible as subgroup of $GL(n/m, \mathbb{E})$ if and only if its centraliser in $GL(n/m, \mathbb{E})$ is $A$.

**2.5.16 Theorem.** (see Suprunenko (1976, Theorem 20.1(iii), Lemmas 20.2 and 20.3, pp. 138-140)) *$F$ is absolutely irreducible as subgroup of $GL(n/m, \mathbb{E})$.* ■

The above theorem is very important, because it implies the following very useful structure theorem for $F$. Although Suprunenko (1976) does not prove this theorem explicitly, it can be deduced from his results between Theorem 20.3 and Theorem 20.8 on pages 141-145.

**2.5.17 Theorem.** *Let $\{q_1, q_2, \ldots, q_r\}$ be the set of primes for which the corresponding Sylow subgroups of $F$ are not cyclic. Write $O_{q_i}(F) = O_{q_i}(A)$ Y $E_i$, where $E_i$ is extraspecial of order $q_i^{1+2l_i}$, and set $F_i := AE_i$. Let $\bar{F}_i$ be an absolutely irreducible subgroup of $GL(q_i^{l_i}, \mathbb{E})$ that is isomorphic to $F_i$ (see Theorem 2.4.7). Then $F$ is conjugate in $GL(n/m, \mathbb{E})$ to $\bar{F}_1 \otimes \ldots \otimes \bar{F}_r$. In particular, $n/m = q_1^{l_1} \ldots q_r^{l_r}$, and $F/A$ is elementary abelian of order $n^2/m^2$.* ■

**2.5.18 Remark.** (see Suprunenko (1976, Corollary 20.3.1, p. 141)) If $q_i$ is a prime that divides $n/m$, then $O_{q_i}(F)$ is not cyclic, and so for the central product $O_{q_i}(A)$ Y $E_i$ to make sense in the above theorem, there must be an element of order $q_i$ in $A$. Therefore we have the condition that every prime which divides $n/m$ must also divide $p^{km} - 1$. This gives a useful restriction on the values that $m$ may take.

The proof of Theorem 2 in Isaacs (1975) requires only minor modification to become a proof of the following theorem.[2]

**2.5.19 Theorem.** *Let $G$ be a (possibly infinite) group with centre $Z$, and let $H$ be a subgroup of $G$ with the following properties:*

[2] I have extended Isaacs' theorem to infinite groups in order to deal with the case when $Z$ is the multiplicative group of an arbitrary field, as in the general theory developed by Suprunenko.

*(i)* $Z(H) = Z$;

*(ii)* $[H, G] \leq Z$;

*(iii)* $H\mathrm{C}_G(H)/Z$ *is finite;*

*(iv)* $|\mathrm{Hom}(H/Z, Z)| \leq |H/Z|$.

*Then* $G/Z = H/Z \times \mathrm{C}_G(H)/Z$. ■

**2.5.20 Corollary.** *$F/A$ is a completely reducible module for $M$.*

**Proof.** Let $B/A$ be a subgroup of $F/A$ that is normal in $M/A$. By the maximality of $A$, we have that $Z(B) = A$. Then, since $B/A$ is a finite abelian group and $A$ is a finite cyclic group, we also have that $|\mathrm{Hom}(B/A, A)| \leq |B/A|$ (as pointed out by Isaacs). Therefore, by the above theorem, $F/A = B/A \times \mathrm{C}_F(B)/A$, and this establishes the result. ■

**2.5.21 Theorem.** *Let $M_1$ and $M_2$ be primitive maximal soluble subgroups of $L$, each having $A$ as its unique maximal abelian normal subgroup. Let $F_1$ and $F_2$ be the Fitting subgroups of $\mathrm{C}_{M_1}(A)$ and $\mathrm{C}_{M_2}(A)$, respectively. Then $M_1$ is conjugate in $L$ to $M_2$ if and only if*

*(i) there is an element $x \in \mathrm{N}_L(A)$ such that $F_2^x = F_1$;*

*(ii) $M_1/F_1$ is conjugate in $\mathrm{N}_L(F_1)/F_1$ to $M_2^x/F_1$.*

**Proof.** Suppose that $M_2^x = M_1$ for some $x \in L$. Since $M_1$ and $M_2$ have the same unique maximal abelian normal subgroup $A$, it follows that $x \in \mathrm{N}_L(A)$. Since $A$ uniquely determines $F_1$ in $M_1$ and $F_2$ in $M_2$, properties (i) and (ii) follow.

Conversely, suppose that (i) and (ii) hold. If $yF_1$ is an element of $\mathrm{N}_L(F_1)/F_1$ that conjugates $M_2^x/F_1$ to $M_1/F_1$, then it is clear that $y$ conjugates $M_2^x$ to $M_1$. ■

This theorem makes it clear that the group $\mathrm{N}_L(F)/F$ is of great importance. Its structure is known (for the structure of $\mathrm{N}_{GL(n/m,\mathbb{E})}(F)/F$, see Suprunenko (1976, Theorems 20.13-16, pp. 149-151)) but is messy to describe, and we do not attempt it. Furthermore, there is no known useful 'construction theorem' in

the general case. That is, there is no known practical theorem that tells us how to construct a complete set of conjugacy class representatives of the primitive maximal soluble subgroups of $L$. (We can always begin with all maximal soluble subgroups of $\mathbf{N}_L(F)/F$ (but how does one find them?) and pull them back, but this is not very helpful.) Therefore we introduce a restriction so that the presentation can be made complete: we will assume that $n/m$ is a prime power. The least value of $n$ for which this assumption could fail is 6; by Remark 2.5.18, however, we would also require $p^k \equiv 1 \bmod 6$. In particular, the theory we develop is sufficient to identify the primitive maximal soluble subgroups of $GL(n, p^k)$ for $p^{kn} < 7^6 = 117\,649$.

**2.5.22 Remark.** If $m = n$, then $A$ is a Singer cycle of $L$, and $M$ is a subgroup of its normaliser. By Theorem 2.3.5 that normaliser is soluble, and so equals $M$. A method of constructing the normaliser of a Singer cycle was given in Section 2.3. Also, the normalisers of the Singer cycles form a single conjugacy class (see Theorem 2.3.3) and therefore it is sufficient to construct just one.

**2.5.23 Notation.** Assume $n/m = q^l$, where $q$ is a prime divisor of $p^{km} - 1$ and $l > 0$ (that is, $m < n$). Define $E$ by $F = A \curlyvee E$, where $E$ is extraspecial of order $q^{1+2l}$ and exponent $q$ or 4, and where $O_2(F) \ncong D_8$.

First we fix a generating set for $F$.

**2.5.24 Notation.** Set $\varepsilon := \bar{z}^{(p^{km}-1)/q}$, and fix $\alpha$ and $\beta$ to be two elements of $\mathbb{F}I_m$ such that $\alpha^2 + \beta^2 = -I_m$.

With this notation established, we define the $n$ by $n$ matrices $u_1, v_1, \ldots, u_l, v_l$ as in Section 2.4 (page 20). Recall that the definitions of $u_l$ and $v_l$ may depend on the isomorphism type of $E$. Then, by construction, $F$ is (abstractly) isomorphic to $\langle u_1, v_1, \ldots, u_l, v_l, z\rangle$. By Theorem 2.4.7, we conclude that $F$ is conjugate in $GL(n/m, \mathbb{E})$ to $\langle u_1, v_1, \ldots, u_l, v_l, z\rangle$. Therefore, without loss of generality, we can conjugate $M$ so that $F = \langle u_1, v_1, \ldots, u_l, v_l, z\rangle$, and so that $M$ remains a subgroup of $\mathbf{N}_L(A)$.

Before investigating $M/F$, we must discuss $\mathbf{N}_L(F)/F$.

**2.5.25 Notation.** Let $a$ be the matrix of $\mathbf{N}_L(A)$ that was constructed in the proof of Theorem 2.5.13, and let $N$ be the normaliser in $GL(n/m, \mathbb{E})$ of $F$.

The isomorphism type of $N/F$ is given by Theorem 2.4.12. It is clear that $\mathbf{N}_L(F) \leq \mathbf{N}_L(A)$, and therefore $\mathbf{N}_L(F)/N$ is cyclic of order dividing $m$ (see Theorem 2.5.13). The next theorem shows that the order of this group is in fact equal to $m$.

**2.5.26 Theorem.** $\mathbf{N}_L(F) = N \rtimes \langle a \rangle$. *The action of $a$ is $p^k$-th powering on each $m$ by $m$ block of $N$.*

**Proof.** It is easy to verify that $u_i^a = u_i$ and $v_i^a = v_i^{p^k}$, except that if $F$ has type III(b), then $v_l^a = v_l$. Therefore $a$ normalises $F$. Since $\langle a \rangle \cap \mathbf{C}_L(A)$ is trivial, the result follows. ■

**2.5.27 Theorem.** *The centraliser in $\mathbf{N}_L(F)$ of $F/A$ is $F\mathbf{C}_{\langle a \rangle}(v_1, \ldots, v_l)$.*

**Proof.** Take any element $bg \in \mathbf{N}_L(F)$, where $b \in \langle a \rangle$ and $g \in N$, and suppose that $bg$ centralises $F/A$. Then, in particular, $bg$ fixes (set-wise) each $Au_i$. Since $b$ fixes $u_i$, it follows that $g$ fixes $Au_i$. Now $(Av_i)^b$ is a power of $Av_i$, say $(Av_i)^s$, and therefore $(Av_i)^g = (Av_i)^{s^{-1}}$ where by $s^{-1}$ we mean the inverse of $s$ modulo $q$. Then $[v_i, u_i]^g = [v_i, u_i]^{s^{-1}}$. Since $g \in \mathbf{C}_L(A)$ and $F' \leq A$, we conclude that $s = 1$, that is, both $b$ and $g$ fix $Av_i$. Therefore,

$$\mathbf{C}_{\mathbf{N}_L(F)}(F/A) = \mathbf{C}_N(F/A)\mathbf{C}_{\langle a \rangle}(F/A)\,.$$

From Theorem 2.4.13 we deduce that $\mathbf{C}_N(F/A) = F$ and it is easy to verify that $\mathbf{C}_{\langle a \rangle}(F/A) = \mathbf{C}_{\langle a \rangle}(v_1, \ldots, v_l)$. ■

**2.5.28 Notation.** Define the map $\rho : \mathbf{N}_L(F) \to GL(2l, q)$ by

$$g\rho := \begin{pmatrix} \alpha_{11} & \beta_{11} & \ldots & \alpha_{1l} & \beta_{1l} \\ \gamma_{11} & \delta_{11} & \ldots & \gamma_{1l} & \delta_{1l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{l1} & \beta_{l1} & \ldots & \alpha_{ll} & \beta_{ll} \\ \gamma_{l1} & \delta_{l1} & \ldots & \gamma_{ll} & \delta_{ll} \end{pmatrix},$$

where

$$\begin{aligned} u_i^g &= u_1^{\alpha_{i1}} v_1^{\beta_{i1}} \dots u_l^{\alpha_{il}} v_l^{\beta_{il}} z^{\lambda_i}, \\ v_i^g &= u_1^{\gamma_{i1}} v_1^{\delta_{i1}} \dots u_l^{\gamma_{il}} v_l^{\delta_{il}} z^{\mu_i}, \\ z^g &= z^\nu. \end{aligned}$$

**2.5.29 Theorem.** *The map $\rho$ is a homomorphism whose kernel is $F\mathbf{C}_{\langle a\rangle}(v_1, \dots, v_l)$ and whose image is a semidirect product: the normal factor of the semidirect product is $Sp(2l, q)$, $Sp(2l, 2)$, $O^+(2l, 2)$ or $O^-(2l, 2)$, according as $F$ has type I, II, III(a) or III(b), respectively; the other factor of the semidirect product is the group generated by the block diagonal matrix with the matrix*

$$\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}$$

*running down its diagonal.*

**Proof.** It is routine (but tedious) to verify that $\rho$ is a homomorphism. We already know from Section 2.4 that $N\rho$ equals $Sp(2l, q)$, $Sp(2l, 2)$, $O^+(2l, 2)$ or $O^-(2l, 2)$, according as $F$ has type I, II, III(a) or III(b), respectively. From the proof of Theorem 2.5.26, it is clear that $a\rho$ is the block diagonal matrix with the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}$$

running down its diagonal, even when $F$ has type III(b) (as $p$ is odd in that case). Therefore the image of $\rho$ is as stated. The claim about the kernel of $\rho$ follows from the previous theorem. ∎

**2.5.30 Theorem.** $\mathbf{C}_{\langle a\rangle}(v_1, \dots, v_l) \leq M$.

**Proof.** $F\mathbf{C}_{\langle a\rangle}(v_1, \dots, v_l)$, being the kernel of $\rho$, is normal in $\mathbf{N}_L(F)$, and is clearly soluble. Since $F \leq M \leq \mathbf{N}_L(F)$, it follows that $M\mathbf{C}_{\langle a\rangle}(v_1, \dots, v_l)$ is soluble. The result then follows from the maximality of $M$. ∎

**2.5.31 Definition.** Let $V$ be a vector space admitting a non-degenerate symplectic form. An *isotropic subspace* of $V$ is a subspace on which the symplectic form vanishes.

**2.5.32 Theorem.** *$M\rho$ is a completely reducible maximal soluble subgroup of* $\operatorname{im}\rho$ *that does not fix any non-zero isotropic subspace of $F/A$.*

**Proof.** Let $P\rho$ be a maximal soluble subgroup of $\operatorname{im}\rho$ that contains $M\rho$, and let $P$ be the complete inverse image of $P\rho$ (that is, $P$ is the subgroup generated by all the inverse images of $P\rho$). Since $P\rho \geq M\rho$, it follows that $P \geq M$, and since both $\ker\rho$ and $P\rho$ are soluble, it follows that $P$ is soluble. The maximality of $M$ then gives us that $P = M$. Therefore $M\rho$ is a maximal soluble subgroup of $\operatorname{im}\rho$. By Corollary 2.5.20, $M\rho$ is completely reducible. Finally, if $B/A$ is an isotropic subspace of $F/A$ that is fixed by $M\rho$, then $B$ is an abelian normal subgroup of $M$. The maximality of $A$ then gives us that $B = A$. ∎

The next two theorems are among the most important in the whole thesis: they tell us how to construct a complete set of conjugacy class representatives of the primitive maximal soluble subgroups of $GL(n, \mathbb{F})$ whose unique maximal abelian normal subgroup has order $p^{km} - 1$, where $n/m$ is a prime power.

**2.5.33 Theorem.** *Let $n = q^l m$, where $l > 0$ and $q$ is a prime divisor of $p^{km} - 1$. If $q = 2$, then suppose in addition that $p^{km} \equiv 1 \bmod 4$. Let $\bar{z}$ be our fixed generator of a Singer cycle of $GL(m, \mathbb{F})$, and let $\bar{a}$ be our fixed element of order $m$ in $GL(m, \mathbb{F})$ such that $\bar{a}^{-1}\bar{z}\bar{a} = \bar{z}^{p^k}$. Let $a$ and $z$ be the $n$ by $n$ block diagonal matrices with $\bar{a}$ and $\bar{z}$ running down their diagonals, respectively. Define the matrices $u_i$ and $v_i$ as above. Let $S$ be the subgroup of $GL(2l, q)$ that is generated by $Sp(2l, q)$ and the block diagonal matrix with the matrix*

$$\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}$$

*running down its diagonal. Let $D$ be a completely reducible (not necessarily maximal) soluble subgroup of $S$ which does not fix any non-zero isotropic subspace of the natural module for $Sp(2l, q)$. Suppose $D$ has generating set $\{d_1, \ldots, d_r\}$. If $d_i$*

*is the matrix*

$$\begin{pmatrix} \alpha_{11} & \beta_{11} & \dots & \alpha_{1l} & \beta_{1l} \\ \gamma_{11} & \delta_{11} & \dots & \gamma_{1l} & \delta_{1l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{l1} & \beta_{l1} & \dots & \alpha_{ll} & \beta_{ll} \\ \gamma_{l1} & \delta_{l1} & \dots & \gamma_{ll} & \delta_{ll} \end{pmatrix},$$

*then let $g_i$ be any matrix of $GL(n, \mathbb{F})$ satisfying*

$$\begin{aligned} u_j^{g_i} &= u_1^{\alpha_{j1}} v_1^{\beta_{j1}} \dots u_l^{\alpha_{jl}} v_l^{\beta_{jl}} z^{\lambda_j}, \\ v_j^{g_i} &= u_1^{\gamma_{j1}} v_1^{\delta_{j1}} \dots u_l^{\gamma_{jl}} v_l^{\delta_{jl}} z^{\mu_j}, \end{aligned}$$

*for some (arbitrary) integers $\lambda_j$ and $\mu_j$. Let $P$ be the subgroup of $GL(n, \mathbb{F})$ defined by*

$$P := \langle \mathbf{C}_{\langle a \rangle}(v_1, \dots, v_l), g_1, \dots, g_r, u_1, v_1, \dots, u_l, v_l, z \rangle.$$

*Then $P$ is the complete inverse image of $D$ under $\rho$. Furthermore, $P$ is primitive and has a maximal abelian normal subgroup of order $p^{km} - 1$. Now let $\mathcal{D}$ be a complete and irredundant set of $S$-conjugacy class representatives of the completely reducible maximal soluble subgroups of $S$ which do not fix any non-zero isotropic subspace of the natural module for $Sp(2l, q)$. Let $\mathcal{P}$ be the set of groups $P$ obtained by the above method, one for each $D$, where $D$ runs through the members of $\mathcal{D}$. No two members of $\mathcal{P}$ are conjugate in $GL(n, \mathbb{F})$. If $M$ is a primitive maximal soluble subgroup of $GL(n, \mathbb{F})$ whose unique maximal abelian normal subgroup has order $p^{km} - 1$, then $M$ is conjugate to a member of $\mathcal{P}$.*

**Proof.** Denote $\langle z \rangle$ by $A$, $\langle u_1, v_1, \dots, u_l, v_l, z \rangle$ by $F$, and $GL(n, \mathbb{F})$ by $L$. We will be using several of the theorems about $A$ and $F$ given in this section, but notice that they are independent of $M$.

There is a matrix $g_i$ satisfying the above requirements because $d_i$ comes from $\operatorname{im} \rho$. By construction, $P$ is the complete inverse image of $\rho$. (It is an inverse image, and contains $\ker \rho$.) No two members of $\mathcal{P}$ can be conjugate in $L$ because their images under $\rho$ are not conjugate in $S$. It is clear that $P$ is soluble.

First we show that $P$ is irreducible. We know from Theorem 2.5.13 that $\mathbf{C}_L(A) = GL(q^l, \mathbb{E})$, and from Theorem 2.4.7 that $F$ is absolutely irreducible

as subgroup of $GL(q^l, \mathbb{E})$. Let $N$ be the normaliser in $GL(q^l, \mathbb{E})$ of $F$. From Theorem 2.5.26 we have that $\mathbf{N}_L(F) = \langle a, N \rangle$. Therefore $\mathbf{C}_L(F) = A$, because $\mathbf{C}_{\langle a \rangle}(z) = 1$. By Maschke's Theorem, $F$ is completely reducible as subgroup of $L$. Let $U$ be the natural $\mathbb{F}F$-module, and suppose that $U = V \oplus W$, where $V$ and $W$ are non-zero $\mathbb{F}F$-submodules of $U$. Since the linear span, $\mathbb{K}$, of $A$ is a field, and since $Z(F) = A$, we may view $U$, $V$ and $W$ as (non-zero) $\mathbb{K}F$-modules. But then $\mathbf{C}_L(F)$ contains (as abstract group) $\mathbb{K}^{\times} \times \mathbb{K}^{\times}$, which equals $A \times A$. This is a contradiction to $\mathbf{C}_L(F) = A$, except when $A = 1$. However, if $A = 1$, then we have a contradiction to $q | (p^{km} - 1)$. Hence $F$ is irreducible as subgroup of $L$. Therefore $P$ is irreducible too.

Now we prove that $A$ is a maximal abelian normal subgroup of $P$. Let $B$ be an abelian normal subgroup of $P$ containing $A$. Since $A \leq Z(N)$ and $\mathbf{C}_{\langle a \rangle}(z) = 1$, we must have $B \leq N$. Then $B \cap F$ is an abelian normal subgroup of $P$ between $A$ and $F$. Since $(B \cap F)/A$ is an isotropic subspace of $F/A$ that admits $D$, we conclude that $B \cap F = A$. Since $BF$ is nilpotent (by Fitting's Theorem), and $A \leq Z(BF)$, we have that $O_{q'}(BF) \leq \mathbf{C}_L(F)$. Since $\mathbf{C}_L(F) = A$, we conclude that $BF/F$ is a $q$-group. So $BF/F$ is a normal $q$-subgroup of $D$. Since $D$ is completely reducible in characteristic $q$, we conclude that $BF = F$, and hence $B = A$. So $A$ is a maximal abelian normal subgroup of $P$.

Now we show that $P$ is primitive. (This part of the proof is due to L. G. Kovács.) Suppose that $P$ is imprimitive. Let $U$ be the natural module for $P$, let $V$ be a block of imprimitivity for $P$, and set $H := \mathbf{N}_P(V)$. Since $U$ is an irreducible $\mathbb{F}P$-module, it follows that $V$ is an irreducible $\mathbb{F}H$-module. We first show that $H \geq A$.

The space $V$ admits $H \cap A$; let $W$ be an irreducible $\mathbb{F}(H \cap A)$-submodule of $V$, and let $W^+$ be the $\mathbb{F}A$-submodule of $U$ generated by $W$. We will show that $W^+$ is faithful, irreducible and has $\mathbb{F}$-dimension $m$. Since $W$ is a direct summand of $\mathrm{Reg}(\mathbb{F}(H \cap A))$ (the regular module for $\mathbb{F}(H \cap A)$), and since

$$\mathrm{Ind}_{H \cap A}^{A}(\mathrm{Reg}(\mathbb{F}(H \cap A))) \cong \mathrm{Reg}(\mathbb{F}A),$$

we conclude that $\mathrm{Ind}_{H \cap A}^{A}(W)$ is a direct summand of $\mathrm{Reg}(\mathbb{F}A)$. But of course $\mathrm{Ind}_{H \cap A}^{A}(W)$ is isomorphic to $W^+$, and so $W^+$ is a direct summand of $\mathrm{Reg}(\mathbb{F}A)$.

Since $\mathrm{Reg}(\mathbb{F}A)$ is multiplicity-free, it follows that $W^+$ is multiplicity-free. Now $W^+$ is a submodule of $U|_A$, and, by construction, $U|_A$ is the direct sum of $n/m$ pairwise isomorphic faithful irreducible $\mathbb{F}A$-modules of dimension $m$. Therefore the only multiplicity-free submodules of $U|_A$ are the irreducible ones, and hence we conclude that $W^+$ is faithful, irreducible, and has $\mathbb{F}$-dimension $m$. Now we show that $W$ and $W^+$ have the same $\mathbb{F}$-dimension. Let $r$ be the $\mathbb{F}$-dimension of $W$; since $\mathrm{Ind}_{H\cap A}^{A}(W)$ is isomorphic to $W^+$, we have that $m = r|A\colon H \cap A|$. Let $\mathrm{sp}(H \cap A)$ be the $\mathbb{F}$-linear span of the elements of $H \cap A$; this span is a subring of the finite field $\mathrm{sp}(A)$ and hence is a field itself, say $\mathbb{L}$. Then $W$ is an $\mathbb{L}(H \cap A)$-module of $\mathbb{L}$-dimension 1. Since $W$ has $\mathbb{F}$-dimension $r$, it follows that $\mathbb{L}$ is a field of $p^{kr}$ elements. Let $B$ be the multiplicative group of $\mathbb{L}$. Since $B \leq A$, we see that $|A\colon B| \leq |A\colon H \cap A|$, that is, $(p^{km} - 1)/(p^{kr} - 1) \leq m/r$. This implies that $r = m$. Therefore $W$ and $W^+$ are equal as vector spaces, which means that $W$ admits $A$. So every irreducible $\mathbb{F}(H \cap A)$-submodule of $V$ admits $A$. Since $H \cap A \trianglelefteq H$, it follows that $V|_{H\cap A}$ is completely reducible. Therefore $V$ admits $A$, and so $H \geq A$.

Since $F$ is irreducible, we have that $P = HF$. Now $H \cap F \trianglelefteq H$, and since $H \cap F \geq A \geq F'$, we have that $H \cap F \trianglelefteq F$. Consequently $H \cap F \trianglelefteq P$. We now show that $V|_{H\cap F}$ is faithful and irreducible. Since $U|_F$ is irreducible, and since $\mathrm{Ind}_{H\cap F}^{F}(V|_{H\cap F}) \cong U|_F$, it follows that $V|_{H\cap F}$ is irreducible. By the maximality of $A$, we have that $Z(H \cap F) = A$. Then by Theorem 2.5.19 we have that $F = (H \cap F)\mathbf{C}_F(H \cap F)$. Since the coset representatives of $H \cap F$ in $F$ centralise $H \cap F$, it follows that $\mathrm{Ind}_{H\cap F}^{F}(V|_{H\cap F})$ is the direct sum of pairwise isomorphic irreducible $\mathbb{F}(H \cap F)$-modules. Since $U|_F$ is faithful, we have that $V|_{H\cap F}$ is faithful.

Let $B$ be an abelian characteristic subgroup of $H \cap F$; then $B$ is an abelian normal subgroup of $P$. Since $A = Z(H \cap F)$, it follows that $BA$ is an abelian normal subgroup of $P$. By the maximality of $A$, we have that $B \leq A$. Therefore, every abelian characteristic subgroup of $H \cap F$ is contained in $A$, that is, is cyclic and central. Hence, by Corollary 2.4.5, we may write $H \cap F = A \curlyvee E$, where $E$ has order $q^{1+2s}$ $(0 \leq s < l)$, and if $s > 0$, then $E$ is extraspecial (and has

exponent $q$ or 4, and $O_2(H \cap F) \ncong D_8$). Note that $s$ cannot equal $l$ because $F$ is irreducible and so cannot normalise $V$. As mentioned in the third paragraph of this proof, we may view $U|_F$ as a $\mathbb{K}F$-module. Since $V|_{H\cap F}$ is a faithful irreducible $\mathbb{F}(H \cap F)$-module, it is also a faithful irreducible $\mathbb{K}(H \cap F)$-module. We know from Theorem 2.4.7 that the $\mathbb{K}$-dimension of $V|_{H\cap F}$ must be $q^s$, and therefore the $\mathbb{F}$-dimension of $V|_{H\cap F}$ is $mq^s$. From this and the fact that $\dim_{\mathbb{F}}(U) = |F: H \cap F|\dim_{\mathbb{F}}(V)$ we conclude that $q^{l-s} = 1$, that is, $s = l$. This contradiction shows that $P$ must be primitive.

We have now shown that every member $P$ of $\mathcal{P}$ is primitive and has a maximal abelian normal subgroup $A$ of order $p^{km} - 1$. If $P$ is maximal soluble, then $A$ is unique, from Theorem 2.5.11e. By combining the earlier theorems of this section, we get a proof that every primitive maximal soluble subgroup of $GL(n, \mathbb{F})$ whose unique maximal abelian normal subgroup has order $p^{km} - 1$ is conjugate to a member of $\mathcal{P}$. ■

**2.5.34 Remark.** Consider the case when $n/m = q$ and $q$ is odd. Then $S$ is the subgroup of $GL(2, q)$ that is generated by $Sp(2, q)$ (which equals $SL(2, q)$) and the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}.$$

We need a complete and irredundant set of $S$-conjugacy class representatives of the completely reducible maximal soluble subgroups of $S$ which do not fix any non-zero isotropic subspace of the natural module for $Sp(2, q)$. Clearly a reducible subgroup of this kind will fix a 1-dimensional subspace, which is certainly isotropic. Therefore we are restricted to looking for a complete and irredundant set of $S$-conjugacy class representatives of the irreducible maximal soluble subgroups of $S$.

**2.5.35 Theorem.** *Let $n = 2^l m$, and suppose that $p^{km} \equiv 3 \bmod 4$. Let $\bar{z}$ be our fixed generator of a Singer cycle of $GL(m, \mathbb{F})$, and let $\bar{a}$ be our fixed element of order $m$ in $GL(m, \mathbb{F})$ such that $\bar{a}^{-1}\bar{z}\bar{a} = \bar{z}^{p^k}$. Let $a$ and $z$ be the $n$ by $n$ block diagonal matrices with $\bar{a}$ and $\bar{z}$ running down their diagonals, respectively. For*

*$1 \leq i \leq l-1$ define the matrices $u_i$ and $v_i$ as above. Define $u_l^+$ and $v_l^+$ by*

$$u_l^+ := \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix} \otimes I_{2^{l-1}} \quad \text{and} \quad v_l^+ := \begin{pmatrix} I_m & 0 \\ 0 & -I_m \end{pmatrix} \otimes I_{2^{l-1}},$$

*and define $u_l^-$ and $v_l^-$ by*

$$u_l^- := \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} \otimes I_{2^{l-1}} \quad \text{and} \quad v_l^- := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} \otimes I_{2^{l-1}},$$

*where $\alpha$ and $\beta$ are two elements of $\mathbb{F}I_m$ such that $\alpha^2 + \beta^2 = -I_m$. Let $D$ be a completely reducible (not necessarily maximal) soluble subgroup of $O^+(2l,2)$ or $O^-(2l,2)$ which does not fix any non-zero isotropic subspace of the natural module for the relevant orthogonal group. Suppose $D$ has generating set $\{d_1, \ldots, d_r\}$. If $d_i$ is the matrix*

$$\begin{pmatrix} \alpha_{11} & \beta_{11} & \ldots & \alpha_{1l} & \beta_{1l} \\ \gamma_{11} & \delta_{11} & \ldots & \gamma_{1l} & \delta_{1l} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{l1} & \beta_{l1} & \ldots & \alpha_{ll} & \beta_{ll} \\ \gamma_{l1} & \delta_{l1} & \ldots & \gamma_{ll} & \delta_{ll} \end{pmatrix},$$

*then let $g_i$ be any matrix of $GL(n,\mathbb{F})$ satisfying*

$$\begin{aligned} u_j^{g_i} &= u_1^{\alpha_{j1}} v_1^{\beta_{j1}} \ldots (u_l^*)^{\alpha_{jl}} (v_l^*)^{\beta_{jl}} z^{\lambda_j}, \\ v_j^{g_i} &= u_1^{\gamma_{j1}} v_1^{\delta_{j1}} \ldots (u_l^*)^{\gamma_{jl}} (v_l^*)^{\delta_{jl}} z^{\mu_j}, \end{aligned}$$

*for some (arbitrary) integers $\lambda_j$ and $\mu_j$, and where the superscript $*$ is replaced by $+$ or $-$, according as $D$ belongs to $O^+(2l,2)$ or $O^-(2l,2)$, respectively. Let $P$ be the subgroup of $GL(n,\mathbb{F})$ defined by*

$$P := \langle \mathbf{C}_{\langle a \rangle}(v_1, \ldots, v_l^*), g_1, \ldots, g_r, u_1, v_1, \ldots, u_l^*, v_l^*, z \rangle.$$

*Then $P$ is the complete inverse image of $D$ under $\rho$. Furthermore, $P$ is primitive and has a maximal abelian normal subgroup of order $p^{km} - 1$. Now let $\mathcal{D}^+$ be a complete and irredundant set of $O^+(2l,2)$-conjugacy class representatives of the completely reducible maximal soluble subgroups of $O^+(2l,2)$ which do not fix any non-zero isotropic subspace of the natural module for $O^+(2l,2)$. Define $\mathcal{D}^-$ similarly, with $O^-(2l,2)$ in place of $O^+(2l,2)$. Let $\mathcal{P}$ be the set of groups $P$*

*obtained by the above method, one for each $D$, where $D$ runs through the members of $\mathcal{D}^+$ and $\mathcal{D}^-$. No two members of $\mathcal{P}$ are conjugate in $GL(n,\mathbb{F})$. If $M$ is a primitive maximal soluble subgroup of $GL(n,\mathbb{F})$ whose unique maximal abelian normal subgroup has order $p^{km}-1$, then $M$ is conjugate to a member of $\mathcal{P}$.*

**Proof.** The proof of this theorem goes exactly the same as that of the previous theorem. ■

**2.5.36 Remark.** Consider the case when $n/m = 2$. Observe that $O^+(2,2)$ has order 2 and so is soluble but not completely reducible. This tallies with the fact that if $A$ has no elements of order 4, then $A \Upsilon D_8$ has an abelian characteristic subgroup not contained in $A$. In other words, $F$ cannot have type III(a) in this case (and so we can write $F = A \Upsilon Q_8$). Since $O^-(2,2) = Sp(2,2)$ and $Sp(2,2)$ is soluble, we see that there is at most one conjugacy class of primitive maximal soluble subgroups of $GL(2m,p^k)$ whose unique maximal abelian normal subgroup has order $p^{km}-1$.

**2.5.37 Remark.** Consider the case when $n = 4$ and $m = 1$. Then, for $S$ running through $\{Sp(4,2), O^+(4,2), O^-(4,2)\}$, we need a complete and irredundant set of $S$-conjugacy class representatives of the completely reducible maximal soluble subgroups of $S$ which do not fix any non-zero isotropic subspace of the natural module for $S$. The subgroups of $O^+(4,2)$ and $O^-(4,2)$ are discussed in Appendix B.

**2.5.38 Definition.** Any group constructed by the methods in this section (see Theorems 2.5.7, 2.5.33 and 2.5.35) will be called a *JS-maximal* (for Jordan-Suprunenko) of $GL(n,\mathbb{F})$. We will also use the terms *JS-imprimitive* and *JS-primitive* to denote imprimitive and primitive JS-maximals, respectively.

Note that every JS-maximal is irreducible and soluble, but not necessarily maximal soluble. The smallest value of $p^{kn}$ for which there are JS-maximals that are not maximal soluble is 9. In $GL(2,3)$ there are three JS-maximals, their orders being 8, 16 and 48. Since the third is $GL(2,3)$ itself, the first two cannot be maximal soluble. For the values of $n$ covered in this thesis it is a general rule

that JS-maximals that are not maximal soluble can occur only for the first few prime powers $p^k$.

We will need a concise way to describe the JS-maximals. For the imprimitives we use

$$P \operatorname{wr} T ,$$

where $P$ and $T$ are as described in Theorem 2.5.7. For the primitives, we use

$$(C_{p^{km}-1} \curlyvee E) \curlywedge D ,$$

where $E$ is extraspecial of order $q^{1+2l}$ and exponent $q$ or 4, and $D$ is as described in Theorem 2.5.33 or 2.5.35. Of course, there may be many (pairwise non-isomorphic) groups with a normal subgroup isomorphic to $C_{p^{km}-1} \curlyvee E$ whose quotient is isomorphic to $D$, but we always mean the one obtained by the construction methods in this section. Also, in some cases we find additional structure in a JS-primitive that can be easily expressed in a decomposition like that above—then we will normally use this second decomposition to denote that group.

For $n \leq 7$, we can provide a numbering of the JS-maximals of $GL(n, \mathbb{F})$. A given irreducible soluble subgroup of $GL(n, \mathbb{F})$ may be conjugate to subgroups of several JS-maximals—to avoid counting such a group more than once in our calculations, we associate it with just one JS-maximal. The following definition states how we do this; the distinction between prime and non-prime degrees for cyclic groups is purely for computational convenience.

**2.5.39 Definition.** Let the JS-maximals of $GL(n, \mathbb{F})$ be $M_1, \ldots, M_m$, and let $G$ be an irreducible soluble subgroup of $GL(n, \mathbb{F})$. If $n$ is prime and $G$ is cyclic, then we define the *guardian* of $G$ to be that JS-maximal which is the normaliser of a Singer cycle. Otherwise the guardian of $G$ is defined to be $M_i$, where $i$ is the least positive integer such that $G$ is $GL(n, \mathbb{F})$-conjugate to a subgroup of $M_i$.

Finally, we discuss what appears to be an error in Jordan's work. Dieudonné (1961, p. xxxvii) suggests that Jordan had proved (at least when $k = 1$) that every JS-primitive $M$ is the semidirect product of $\mathbf{C}_M(A)$ and a cyclic group of order $m$ (see Theorem 2.5.13). The following example shows this not to be the case.

**2.5.40 Example.** Set $n = 14$ and $p^k = 13$. We will now determine the JS-primitives of $GL(14, 13)$. By Remark 2.5.18, the permissible values of $m$ are 2, 7 and 14. Therefore $n/m$ is 1 or a prime, and so our theory is sufficient to deal with this group. For $m = 14$, we get the normaliser of a Singer cycle, a group of order $14(13^{14} - 1)$, the prime factorisation of which is $2^4 3.7^3 29 q_1 q_2$, where the $q_i$ are large primes. For $m = 7$, we again get just one group, because $Sp(2, 2)$ is soluble. This group has order $7.6.2^2(13^7 - 1)$, the prime factorisation of which is $2^5 3^2 7 q_2$. Clearly neither of these groups can be conjugate to a subgroup of the other. Now we treat the case $m = 2$. Since $13 \equiv -1 \bmod 7$, we must find the conjugacy classes of maximal irreducible soluble subgroups of the subgroup $S$ of $GL(2, 7)$ generated by $Sp(2, 7)$ (which equals $SL(2, 7)$) and the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

This group can be easily handled by the CAYLEY function lattice (see page 103). It shows that there are three conjugacy classes[3] of maximal soluble subgroups in $S$. Since their members are $7'$-groups, they are completely reducible, and since they are non-abelian, they are irreducible. So there are three conjugacy classes of maximal irreducible soluble subgroups of $S$. Choose one group from each class, and denote them by $G_1$, $G_2$ and $G_3$. The first group is imprimitive and the other two are primitive. The third group is a subgroup of $SL(2, 7)$ (it will provide the counter-example) but the other two are not. The group $G_1$ has order 24, $G_2$ has order 32 (it is a Sylow 2-subgroup) and $G_3$ has order 48 (it is the binary octahedral group—the double cover of $S_4$ that is not $GL(2, 3)$). So for $m = 2$, there are three JS-primitives: $M_1$, $M_2$ and $M_3$, having orders $24.7^2(13^2 - 1)$, $32.7^2(13^2 - 1)$ and $48.7^2(13^2 - 1)$, respectively, that is, $2^6 3^2 7^3$, $2^8 3.7^3$ and $2^7 3^2 7^3$, respectively. Thus there are a total of five JS-primitives in $GL(14, 13)$, and, by virtue of their orders and the fact that $G_1$ is not conjugate to a subgroup of $G_3$, all of them are maximal soluble. But $G_3$ is a subgroup of $SL(2, 7)$, and so the centraliser in $M_3$ of its unique maximal abelian normal subgroup has index 1,

[3]These classes could also be found by intersecting the JS-maximals of $GL(2, 7)$ (which we explicitly describe in later chapters) with $S$, for $S$ is a normal subgroup of $GL(2, 7)$.

not 2, as Jordan apparently claims. ■

Note that this counter-example arises precisely because the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

induces an (outer) automorphism of $PSL(2,7)$ that interchanges the two conjugacy classes of maximal soluble subgroups isomorphic to $S_4$. This was pointed out to me by L. G. Kovács. The other details of the counter-example are needed only to show that the group $M_3$ constructed from $G_3$ is actually a maximal soluble subgroup of $GL(14,13)$.

# Chapter 3

# The imprimitive soluble subgroups of $GL(2, p^k)$

In this chapter we give a theorem that provides a complete and irredundant list of conjugacy class representatives of the imprimitive soluble subgroups of $GL(2, p^k)$.

## 3.1 The JS-imprimitives of $GL(2, p^k)$

Let $\mathbb{F}$ be the field of $p^k$ elements. By Remark 2.5.5 there are no imprimitive soluble subgroups of $GL(2, 2)$, and so we assume throughout this chapter that $p^k > 2$.

Imprimitive linear groups of prime degree must have a minimal block size of 1. Since both $GL(1, \mathbb{F})$ and $S_2$ are soluble, it follows that there is exactly one JS-imprimitive of $GL(2, \mathbb{F})$, namely

$$M := GL(1, \mathbb{F}) \operatorname{wr} S_2 .$$

This group has order $2(p^k - 1)^2$, and is generated by the matrices

$$a := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad b := \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix},$$

where $\alpha$ is a generator of the multiplicative group of $\mathbb{F}$. In order to obtain a

polycyclic presentation of $M$ we introduce a third element

$$c := b^a = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}.$$

Then a polycyclic presentation for $M$ is

$$\begin{aligned} M := \langle a, b, c \mid\ & a^2 = 1, \\ & b^a = c, \quad b^{p^k-1} = 1, \\ & c^a = b, \quad c^b = c, \qquad c^{p^k-1} = 1 \rangle. \end{aligned}$$

Following the usual terminology for wreath products, we call $\langle a \rangle$ the *top group* and $\langle b, c \rangle$ the *base group*. Denote the base group by $B$.

**3.1.1 Lemma.** *If $G$ is an irreducible subgroup of $M$, then $M = GB$ and $G \cap B$ is normal in $M$.*

**Proof.** It is obvious from the matrices $b$ and $c$ that $B$ is reducible, and therefore $G \not\leq B$. Since $|M\colon B|$ is prime, we must have that $M = GB$. It then follows from the fact that $B$ is abelian and normal in $M$ that $G \cap B \trianglelefteq M$. ∎

This lemma shows that it is important to determine which subgroups of $B$ are normal in $M$. Before proceeding with this, however, we present some notation and results that can be put in a more general context.

## 3.2 Miscellaneous results

**3.2.1 Definition.** Let $X$ be an $\Omega$-group, where $\Omega$ is a set of operators on $X$. A subgroup of $X$ is called an *$\Omega$-subgroup* if it is fixed (set-wise) by $\Omega$. If $Y$ and $Z$ are $\Omega$-subgroups of $X$, and $Z \trianglelefteq Y$, then we call $Y/Z$ an *$\Omega$-section* of $X$. An isomorphism from one $\Omega$-group to another that commutes with the elements of $\Omega$ is called an *$\Omega$-isomorphism.*

The following theorem will be used in many places in this thesis.[1] It is illustrated in Figure 3.1.

[1]There is a clear treatment of this theorem by Remak (1930), who attributed at least some of the theory to Klein and Fricke. Zassenhaus (1958, p. 237, exercise 30) attributed the result to Goursat and Lambek.

**3.2.2 Theorem.** (see Suzuki (1982, 4.19, p. 141)) *Let $X$ be an $\Omega$-group, where $\Omega$ is a set of operators, and let $U$ and $V$ be normal $\Omega$-subgroups of $X$. The set of $\Omega$-subgroups of $X$ which lie between $U \cap V$ and $UV$ is bijective with the set of 5-tuples $(U_1, U_0, V_1, V_0, \theta)$ which satisfy the following conditions:*

*(i) $U_1$ and $U_0$ are $\Omega$-subgroups of $X$ lying between $U \cap V$ and $U$, and $U_0 \trianglelefteq U_1$;*

*(ii) $V_1$ and $V_0$ are $\Omega$-subgroups of $X$ lying between $U \cap V$ and $V$, and $V_0 \trianglelefteq V_1$;*

*(iii) $\theta$ is an $\Omega$-isomorphism from $U_1/U_0$ to $V_1/V_0$.*

*The $\Omega$-subgroup of $X$ to which $(U_1, U_0, V_1, V_0, \theta)$ corresponds under this bijection is $\{uv \in U_1V_1 \mid u \in U_1\,,\ v \in V_1\,,\ (U_0u)\theta = V_0v\}$.* ■

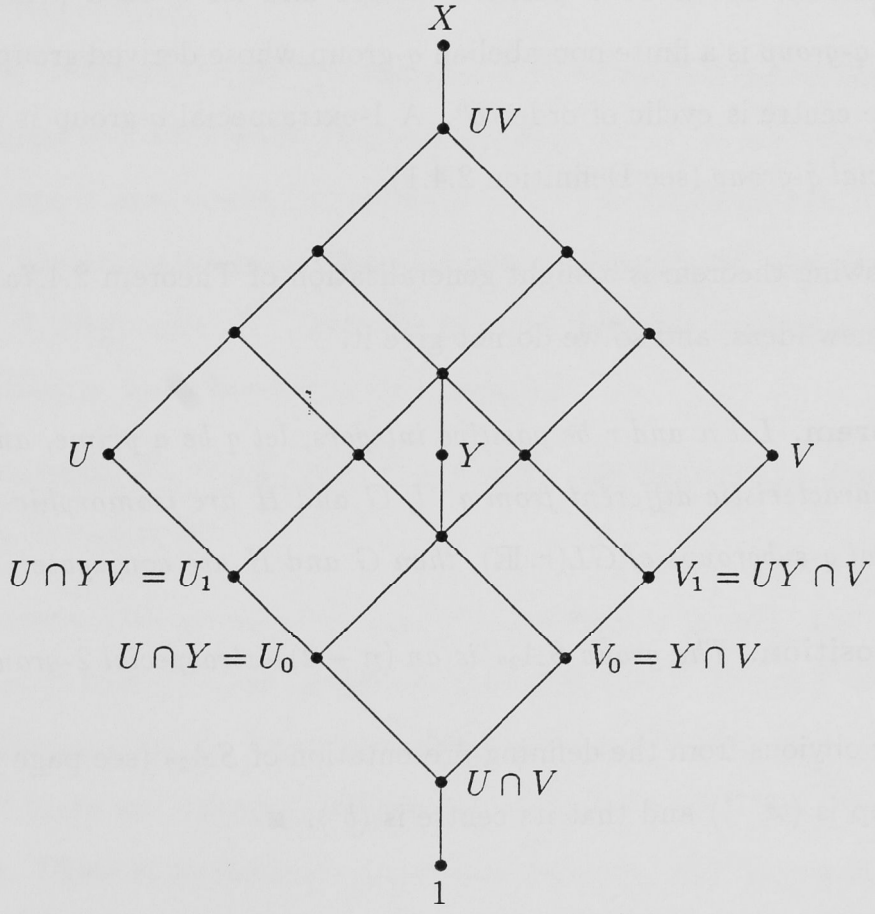



Figure 3.1: Illustration of Theorem 3.2.2

**3.2.3 Definition.** In the notation of Theorem 3.2.2, if $U_0$ is a proper subgroup of $U_1$ (and hence $V_0$ is a proper subgroup of $V_1$), then $Y$ lies properly between $U_0V_0$ and $U_1V_1$, and we call $Y$ a *diagonal $\Omega$-subgroup* of $UV$.

**3.2.4 Notation.** If $G$ is a group and $n$ is a positive integer, we denote by $G^n$ the (characteristic) subgroup of $G$ generated by the $n$-th powers of the elements of $G$.

**3.2.5 Theorem.** (see Huppert (1967, Theorem III.2.6, p. 262)) *If $H$ is a non-trivial normal subgroup of the non-trivial nilpotent group $G$, then $H \cap Z(G) \neq 1$.* ■

**3.2.6 Lemma.** *Let $G$ be a group having a normal subgroup $H$ such that $G/H$ is cyclic of order $n$, say $G = \langle g, H \rangle$, where $g^n \in H$. If there exists an element $h \in \mathrm{C}_H(g)$ such that $h^n = g^n$, then $G$ splits over $H$.*

**Proof.** It is clear that $gh^{-1}$ has order $n$, and that $G = \langle gh^{-1}, H \rangle$. ■

**3.2.7 Definition.** Let $n$ be a positive integer and let $q$ be a prime. An *$n$-extraspecial $q$-group* is a finite non-abelian $q$-group whose derived group has order $q$ and whose centre is cyclic of order $q^n$. A 1-extraspecial $q$-group is also called an *extraspecial $q$-group* (see Definition 2.4.1).

The following theorem is a slight generalisation of Theorem 2.4.7a. Its proof involves no new ideas, and so we do not give it.

**3.2.8 Theorem.** *Let $n$ and $r$ be positive integers, let $q$ be a prime, and let $\mathbb{E}$ be a field of characteristic different from $q$. If $G$ and $H$ are isomorphic irreducible $n$-extraspecial $q$-subgroups of $GL(r, \mathbb{E})$, then $G$ and $H$ are conjugate.* ■

**3.2.9 Proposition.** *The group $SA_{2^n}$ is an $(n-2)$-extraspecial 2-group.*

**Proof.** It is obvious from the defining presentation of $SA_{2^n}$ (see page 6) that its derived group is $\langle b^{2^{n-2}} \rangle$ and that its centre is $\langle b^2 \rangle$. ■

## 3.3 The normal subgroups of $M$ contained in the base group

Let $C$ be a normal subgroup of $M$ contained in $B$. Since $C$ is abelian, it is the direct product of its Sylow subgroups; these subgroups are characteristic in $C$

and so normal in $M$. Conversely, every set of normal subgroups of $M$ that are contained in $B$ and have prime power orders will generate a normal subgroup of $M$ contained in $B$. Therefore the problem of determining all normal subgroups of $M$ that are contained in $B$ is equivalent to the problem of determining all normal $q$-subgroups of $M$ that are contained in $B$, where $q$ runs through the prime divisors of $p^k - 1$.

Let $q$ be a prime divisor of $p^k - 1$. We define $s_q$ to be the integer such that $q^{s_q} \| (p^k - 1)$, and we define $d_q$ and $e_q$ by

$$d_q := b^{(p^k-1)/q^{s_q}} \quad \text{and} \quad e_q := c^{(p^k-1)/q^{s_q}}.$$

Then the Sylow $q$-subgroup of $B$ is $\langle d_q, e_q \rangle$. We denote this group by $T_q$. If it is not necessary to mention $q$ explicitly, then we use $s$, $d$, $e$ and $T$ in place of $s_q$, $d_q$, $e_q$ and $T_q$, respectively.

We wish to determine the $\Omega$-subgroups of $T$, where $\Omega$ is the set comprising the automorphism of $T$ induced by conjugation by $a$. Set $U := \langle de^{-1} \rangle$ and $V := \langle de \rangle$. Clearly $U$ and $V$ are normal $\Omega$-subgroups of $T$. The action of $a$ on $U$ is inverting while on $V$ the action is trivial. Note that every subgroup of $U$ and every subgroup of $V$ is an $\Omega$-subgroup of $T$. Note also that the subgroup lattices of $U$ and $V$ are uniserial (that is, linearly ordered by inclusion).

**3.3.1 Theorem.** *If $q$ is odd, then $T = U \times V$, and there are no diagonals in the $\Omega$-subgroup lattice of $T$.*

**Proof.** Clearly $UV$ contains $d^2$ and $e^2$, and so if $q$ is odd, $UV = T$. Since $|U| = |V| = q^s$ and $|T| = q^{2s}$, it follows that $U \cap V = 1$. Hence $T = U \times V$. We now use Theorem 3.2.2. There are diagonals in the $\Omega$-subgroup lattice of $T$ if and only if there are non-trivial $\Omega$-sections of $U$ and $V$ that are $\Omega$-isomorphic to each other. These $\Omega$-sections are non-trivial $q$-groups, and since $q$ is odd, inverting action is never trivial; hence there can be no non-trivial $\Omega$-sections of $U$ and $V$ that are $\Omega$-isomorphic to each other. Therefore the $\Omega$-subgroup lattice of $T$ contains no diagonals. ■

We have now determined the $\Omega$-subgroup lattice of $T_q$ for $q$ odd. An example is given in Figure 3.2, where we have set $s_q$ to be 2.

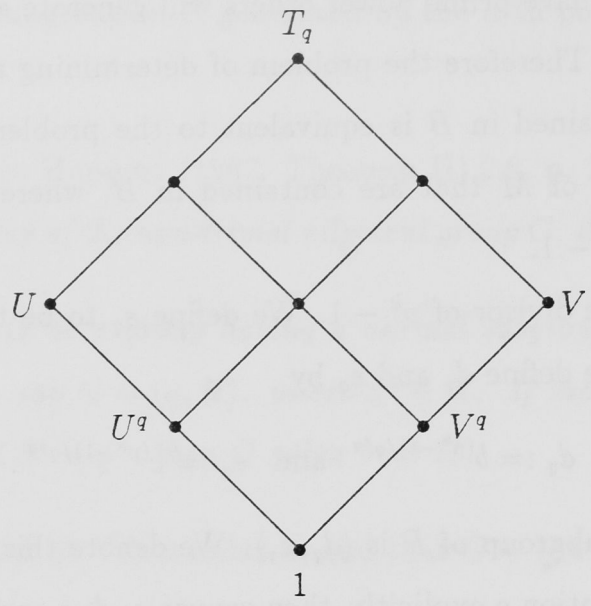


Figure 3.2: The lattice of $\Omega$-subgroups of $T_q$ for $q$ odd and $s_q = 2$

Now suppose that $q = 2$ and that $p$ is odd.

**3.3.2 Theorem.** *$U \cap V = U^{2^{s-1}} = V^{2^{s-1}}$ and is the unique minimal $\Omega$-subgroup of $T$. Also, $UV$ is the unique maximal $\Omega$-subgroup of $T$.*

**Proof.** Obviously $U \cap V = U^{2^{s-1}} = V^{2^{s-1}} = \langle (de)^{2^{s-1}} \rangle$. This group is clearly an $\Omega$-subgroup of $T$, and since it has order 2, it is minimal. It is also clear that $UV = \langle d^2, e^2 \rangle$ and is an $\Omega$-subgroup of $T$, and since it has index 2, it is maximal. Let $G$ be a proper non-trivial $\Omega$-subgroup of $T$. Then $G$ is a non-trivial normal subgroup of the 2-group $\langle a, T \rangle$. It is not difficult to verify that the centre of this group is $V$. By Theorem 3.2.5, $G \cap V \neq 1$, and so $G \geq V^{2^{s-1}}$. Also, if $G$ were not a subgroup of $UV$ then $GUV$ would equal $T$. But then $G$ would contain both $d$ and $e$ (it must contain one of these elements, and it is an $\Omega$-subgroup) and so would be equal to $T$, a contradiction. Hence $G \leq UV$. ■

So apart from the trivial subgroup and $T$ itself, every $\Omega$-subgroup of $T$ lies between $U \cap V$ and $UV$. We now use Theorem 3.2.2. Let $U_1/U_0$ and $V_1/V_0$ be $\Omega$-sections of $U$ and $V$, respectively, lying over $U \cap V$. Clearly $U_1/U_0$ is $\Omega$-isomorphic to $V_1/V_0$ if and only if each section has the same order and that order is 1 or 2, because inversion of a cyclic 2-group is trivial if and only if that 2-group has order 1 or 2. If this order is 1, then the $\Omega$-subgroup is $U_1V_1$. If the order is 2,

then the $\Omega$-subgroup is a diagonal between $U_0V_0$ and $U_1V_1$. Since there is exactly one isomorphism of a group of order 2 with itself, there is only one such diagonal, namely

$$\langle (de^{-1})^{2^i}, (de)^{2^j}, (de^{-1})^{2^{i-1}}(de)^{2^{j-1}} \rangle ,$$

where $U_0 = U^{2^i}$ and $V_0 = V^{2^j}$. Therefore we have determined the $\Omega$-subgroup lattice of $T_2$. An example is given in Figure 3.3, where we have set $s_2$ to be 3.

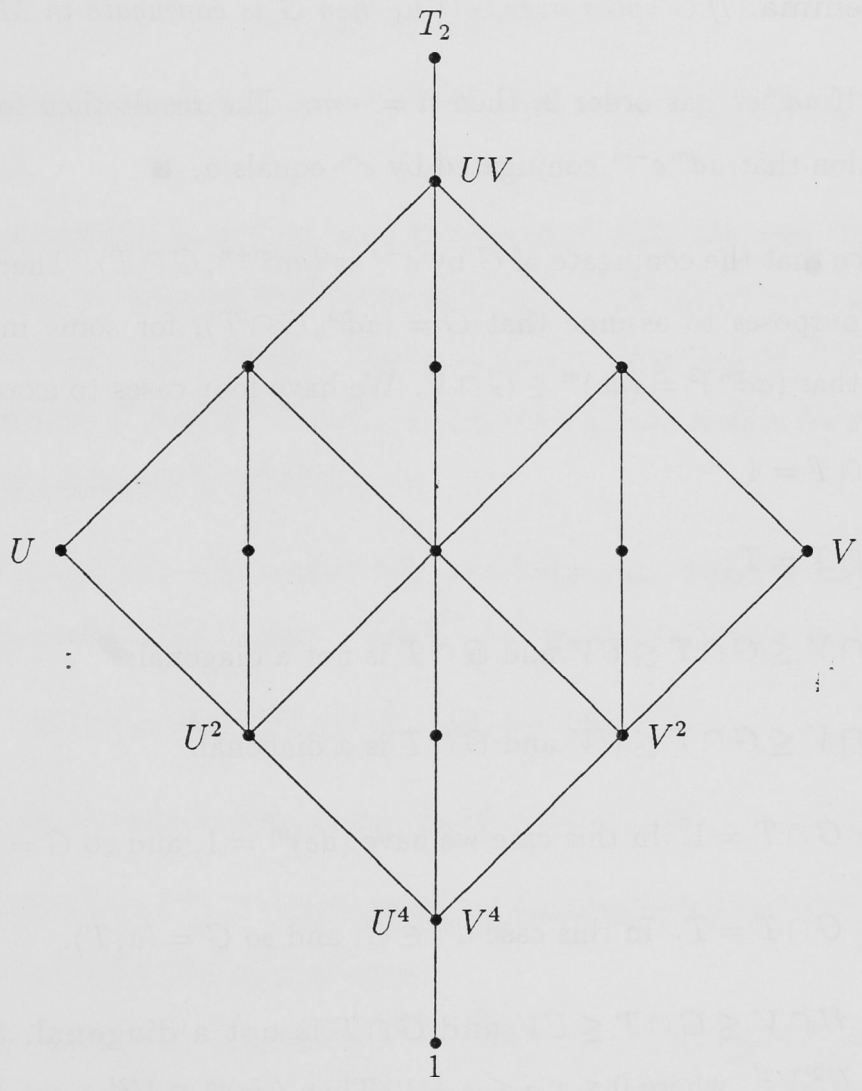



Figure 3.3: The lattice of $\Omega$-subgroups of $T_2$ when $s_2 = 3$

## 3.4 The 2-subgroups of $M$ not contained in $B$

In this section we find a complete and irredundant set of $GL(2, \mathbb{F})$-conjugacy class representatives of the 2-subgroups of $M$ not contained in $B$. We use $d$,

$e$ and $T$ in place of $d_2$, $e_2$ and $T_2$, respectively. Note that Conlon (1977) has determined the non-abelian $q$-subgroups ($q$ prime) of the general linear group of degree $q$ over an arbitrary field. We do not use his results because we wish to describe these groups as subgroups of $M$.

Let $G$ be a 2-subgroup of $M$ not contained in $B$. By the proof of Lemma 3.1.1, $M = GB$ and $G \cap B \trianglelefteq M$. Let $ad^m e^n$ be an element of $G$ not contained in $B$; then $G = \langle ad^m e^n, G \cap T \rangle$.

**3.4.1 Lemma.** *If $G$ splits over $G \cap T$, then $G$ is conjugate in $M$ to $\langle a, G \cap T \rangle$.*

**Proof.** If $ad^m e^n$ has order 2, then $n = -m$. The result then follows from the observation that $ad^m e^{-m}$ conjugated by $e^m$ equals $a$. ∎

Notice that the conjugate of $G$ by $e^{-n}$ is $\langle ad^{m+n}, G \cap T \rangle$. Therefore it suffices for our purposes to assume that $G = \langle ad^m, G \cap T \rangle$, for some integer $m$. Now observe that $(ad^m)^2 = (de)^m \in G \cap V$. We have four cases to examine:

1. $G \cap T = 1$;
2. $G \cap T = T$;
3. $U \cap V \leq G \cap T \leq UV$ and $G \cap T$ is not a diagonal;
4. $U \cap V \leq G \cap T \leq UV$ and $G \cap T$ is a diagonal.

**Case 1:** $G \cap T = 1$. In this case we have $(de)^m = 1$, and so $G = \langle a \rangle$.

**Case 2:** $G \cap T = T$. In this case $d^m \in G$, and so $G = \langle a, T \rangle$.

**Case 3:** $U \cap V \leq G \cap T \leq UV$ **and** $G \cap T$ **is not a diagonal.** Suppose that $G \cap T = U^{2^i} V^{2^j}$, where $0 \leq i, j \leq s - 1$. Then $(de)^m \in V^{2^j}$.

**3.4.2 Lemma.** *In Case 3, if $(de)^m$ generates a proper subgroup of $V^{2^j}$, then $G$ is conjugate in $M$ to $\langle a, G \cap T \rangle$.*

**Proof.** If $(de)^m$ generates a proper subgroup of $V^{2^j}$, then there is an element of $V^{2^j}$ whose square is $(de)^m$. Since $G$ centralises $V$, it then follows from Lemmas 3.2.6 and 3.4.1 that $G$ is conjugate in $M$ to $\langle a, G \cap T \rangle$. ∎

**3.4.3 Lemma.** *In Case 3, if $(de)^m$ generates $V^{2^j}$, then $G$ is conjugate in $M$ to $\langle ad^{2^j}, G \cap T \rangle$, and $G$ is not conjugate in $GL(2, \mathbb{F})$ to $\langle a, G \cap T \rangle$.*

**Proof.** Set $H := \langle ad^{2^j}, G \cap T \rangle$. Writing $m = 2^r n$, where $n$ is odd, we have $\langle (de)^{2^r n} \rangle = \langle (de)^{2^j} \rangle$. Then it is clear that $r = j$. Since $n$ is odd, we have that $H = \langle (ad^{2^j})^n, G \cap T \rangle$. Observe that

$$\begin{aligned} (ad^{2^j})^n &= ad^{2^j}((ad^{2^j})^2)^{(n-1)/2} \\ &= ad^{2^j}((de)^{2^j})^{(n-1)/2} \\ &= ad^{2^j(n+1)/2} e^{2^j(n-1)/2}, \end{aligned}$$

and conjugating this last element by $e^{-2^j(n-1)/2}$ gives $ad^{2^j n}$, which shows that $H$ is conjugate to $G$.

Some easy calculations show that every element of $H$ that has order 2 belongs to $G \cap T$. Therefore the number of elements of order 2 in $H$ equals the number of elements of order 2 in $G \cap T$. Since $a$ has order 2, it is clear that $\langle a, G \cap T \rangle$ has more elements of order 2 than $H$. Therefore, these two groups are not isomorphic, and so cannot be conjugate in $GL(2, \mathbb{F})$. ∎

**Case 4: $U \cap V \leq G \cap T \leq UV$ and $G \cap T$ is a diagonal.** Suppose that $G \cap T$ is the diagonal between $U^{2^i} V^{2^j}$ and $U^{2^{i-1}} V^{2^{j-1}}$, where $1 \leq i, j \leq s - 1$. Then

$$G \cap T = \langle (de^{-1})^{2^i}, (de)^{2^j}, (de^{-1})^{2^{i-1}} (de)^{2^{j-1}} \rangle .$$

**3.4.4 Lemma.** *In Case 4, $G$ is conjugate in $M$ to $\langle a, G \cap T \rangle$.*

**Proof.** Clearly $G \cap V = V^{2^j}$. If $(de)^m$ generates a proper subgroup of $V^{2^j}$, then the proof of Lemma 3.4.2 also applies here.

Now suppose that $(de)^m$ generates $V^{2^j}$. Then, by following the first part of the proof of Lemma 3.4.3, we can assume without loss of generality that $G = \langle ad^{2^j}, G \cap T \rangle$. Since $G \cap T$ contains $(de^{-1})^{2^{i-1}} (de)^{2^{j-1}}$, it follows that $G$ is generated by $G \cap T$ and the element

$$ad^{2^j} (de^{-1})^{2^{i-1}} (de)^{2^{j-1}} .$$

The square of this element is $(de)^{2^{j+1}}$, which generates a proper subgroup of $V^{2^j}$. The result then follows from Lemmas 3.2.6 and 3.4.1. ∎

By combining all of the lemmas in this section so far, we get the following theorem.

**3.4.5 Theorem.** *For odd $p$, the following subgroups of $M$ form a complete and irredundant set of $M$-conjugacy class representatives of the 2-subgroups of $M$ not contained in $B$:*

$$\begin{aligned}
&\langle a\rangle\,;\\
&\langle a, T\rangle\,;\\
&\langle a, N\rangle\,, \qquad N \trianglelefteq M,\quad U\cap V \le N \le UV\,;\\
&\langle ad^{2^j}, N\rangle\,, \quad N \trianglelefteq M,\quad U\cap V \le N \le UV,\quad N\cap V = V^{2^j}\,;\\
&\langle a, D\rangle\,, \qquad D \trianglelefteq M,\quad U\cap V \le D \le UV\,.
\end{aligned}$$

*In this list $D$ and $N$ stand for diagonal and non-diagonal subgroups, respectively.* ■

Let us denote by $\mathcal{S}$ the set in the above theorem. We now refine $\mathcal{S}$ so that no two of its members are conjugate in $GL(2,\mathbb{F})$. First note that neither $\langle a\rangle$ nor $\langle a, T\rangle$ is $GL(2,\mathbb{F})$-conjugate to any other group in $\mathcal{S}$ (by virtue of their orders).

**3.4.6 Proposition.** *Let $G$ and $H$ be members of $\mathcal{S}$ which are conjugate in $GL(2,\mathbb{F})$, and such that $G\cap T \neq H\cap T$. Then one of $G\cap T$ and $H\cap T$ is a diagonal and the other is the non-diagonal of the same order and to its immediate left in the $\Omega$-subgroup lattice of $T$ (writing $U$ on the left, that is, as in Figure 3.3).*

**Proof.** Since $V$ is a subgroup of the scalar group, it is fixed element-wise by conjugation. Therefore $G\cap V = H\cap V$. Since $G\cap T$ and $H\cap T$ must have the same order, the only possibility is that listed in the proposition. ■

**3.4.7 Lemma.** *If $N_1$ and $N_2$ are non-diagonals lying between $U\cap V$ and $UV$, then $\langle a, N_1\rangle$ and $\langle ad^{2^j}, N_2\rangle$ are not conjugate in $GL(2,\mathbb{F})$.*

**Proof.** This follows from Lemma 3.4.3 and Proposition 3.4.6. ■

In the next two lemmas we assume that $N = U^{2^i}V^{2^j}$, $0 \le i,j \le s-1$, and that $D$ is the diagonal between $U^{2^m}V^{2^n}$ and $U^{2^{m-1}}V^{2^{n-1}}$, $1 \le m,n \le s-1$. We

will determine under what conditions any of the groups $\langle a, N\rangle$, $\langle ad^{2^j}, N\rangle$ and $\langle a, D\rangle$ are $GL(2, \mathbb{F})$-conjugate. First observe that

$$\begin{aligned}\langle a, D\rangle &= \langle a, (de^{-1})^{2^m}, (de)^{2^n}, (de^{-1})^{2^{m-1}}(de)^{2^{n-1}}\rangle \\ &= \langle a, (de^{-1})^{2^m}, (de^{-1})^{2^{m-1}}(de)^{2^{n-1}}\rangle .\end{aligned}$$

**3.4.8 Lemma.** *If $i = s-1$, then $\langle a, N\rangle \cong C_{2^{s-j}} \times C_2$. If $i < s-1$, then $\langle a, N\rangle \cong C_{2^{s-j}} \curlyvee D_{2^{s-i+1}}$.*

**Proof.** This is clear. ∎

**3.4.9 Lemma.** *If $m = n = s-1$, then $\langle a, D\rangle \cong D_8$. If $m < n = s-1$, then $\langle a, D\rangle \cong SD_{2^{s-m+2}}$.*

**Proof.** If $m = n = s-1$, then the result is easily checked. If $m < n = s-1$, then

$$\begin{aligned}\langle a, D\rangle &= \langle a, (de^{-1})^{2^m}, (de^{-1})^{2^{m-1}}(de)^{2^{s-2}}\rangle \\ &= \langle a, (de^{-1})^{2^{m-1}}(de)^{2^{s-2}}\rangle .\end{aligned}$$

It is straight-forward to check that the element $(de^{-1})^{2^{m-1}}(de)^{2^{s-2}}$ has order $2^{s-m+1}$ and that its conjugate by $a$ equals its $(-1+2^{s-m})$-th power. ∎

**3.4.10 Lemma.** *$\langle a, N\rangle$ is $GL(2, \mathbb{F})$-conjugate to $\langle a, D\rangle$ if and only if $i+1$, $j$, $m$ and $n$ all equal $s-1$. In this case both groups are isomorphic to $D_8$.*

**Proof.** Suppose that $\langle a, N\rangle$ is $GL(2, \mathbb{F})$-conjugate to $\langle a, D\rangle$. Then by Proposition 3.4.6, $m-1 = i \leq s-2$ and $n = j \geq 1$. Since $\langle a, N\rangle$ and $\langle a, D\rangle$ are conjugate, they are also isomorphic. Note that $\langle a, D\rangle$ can be generated by two elements. From Lemma 3.4.8, if $\langle a, N\rangle$ can be generated by two elements, then at least one of $i$ and $j$ equals $s-1$. If $i = s-1$, then $m = s$ and $\langle a, D\rangle$ is not defined. Therefore $i < j = s-1$. Hence $\langle a, N\rangle$ is isomorphic to $D(2^{s-i+1})$, and $\langle a, D\rangle$ is isomorphic to $D_8$ or $SD(2^{s-i+1})$ according as $i$ equals or is less than $s-2$, respectively. Therefore $i = s-2$.

Conversely, suppose that $i+1$, $j$, $m$ and $n$ all equal $s-1$. Then both $\langle a, N\rangle$ and $\langle a, D\rangle$ are isomorphic to $D_8$. These groups, being completely reducible by Maschke's Theorem, and non-abelian groups of degree 2, must be irreducible. Since $D_8$ is extraspecial, $\langle a, N\rangle$ and $\langle a, D\rangle$ are conjugate in $GL(2, \mathbb{F})$, by Theorem 2.4.7a. ∎

**3.4.11 Lemma.** *If $j \leq i = s-2$, then $\langle ad^{2^j}, N\rangle \cong SA_{2^{s-j+2}}$* (see page 6).

**Proof.** Under the assumptions about $i$ and $j$, we have

$$\langle ad^{2^j}, N\rangle = \langle ad^{2^j}, (de^{-1})^{2^{s-2}}\rangle .$$

Denote the first element in this description by $y$ and the second by $x$. It is straight-forward to check that $y$ has order $2^{s-j+1}$, and that its conjugate by $x$ is its $(1+2^{s-j})$-th power. The result then follows from the fact that $xy^{2^{s-j-1}}$ has order 2. ■

**3.4.12 Lemma.** *If $n < m = s-1$, then $\langle a, D\rangle \cong SA_{2^{s-n+2}}$.*

**Proof.** Under the assumptions about $m$ and $n$, we have

$$\langle a, D\rangle = \langle a, (de^{-1})^{2^{s-2}}(de)^{2^{n-1}}\rangle .$$

It is straight-forward to check that the element $(de^{-1})^{2^{s-2}}(de)^{2^{n-1}}$ has order $2^{s-n+1}$ and that its conjugate by $a$ equals its $(1+2^{s-n})$-th power. ■

**3.4.13 Lemma.** *$\langle ad^{2^j}, N\rangle$ is $GL(2,\mathbb{F})$-conjugate to $\langle a, D\rangle$ if and only if*

*(i)* $m-1 = i = s-2$, *and*

*(ii)* $1 \leq n = j \leq s-2$.

*In this case both groups are isomorphic to $SA_{2^{s-j+2}}$.*

**Proof.** Suppose that $\langle ad^{2^j}, N\rangle$ is $GL(2,\mathbb{F})$-conjugate to $\langle a, D\rangle$. Then by Proposition 3.4.6, $m-1 = i \leq s-2$ and $n = j \geq 1$. Since $\langle ad^{2^j}, N\rangle$ and $\langle a, D\rangle$ are conjugate, they are also isomorphic. As was mentioned in the proof of Lemma 3.4.3, every element of order 2 in $\langle ad^{2^j}, N\rangle$ lies in $N$. Therefore $\langle ad^{2^j}, N\rangle$ contains exactly three elements of order 2, except when $N$ is cyclic, in which case it has just one element of order 2. On the other hand, if $D$ is not cyclic, then $\langle a, D\rangle$ has at least four elements of order 2. Hence $D$ is cyclic, which implies that $i+1$ or $j$ equals $s-1$. If $j = s-1$, then $\langle ad^{2^j}, N\rangle$ has exactly one element of order 2, whereas $\langle a, D\rangle$ has at least two. Therefore $j \leq i = s-2$.

Conversely, suppose that $m-1=i=s-2$, and $1 \leq n=j \leq s-2$. Then both $\langle ad^{2^j}, N\rangle$ and $\langle a, D\rangle$ are isomorphic to $SA_{2^{s-j+2}}$. These groups, being completely reducible by Maschke's Theorem, and non-abelian groups of degree 2, must be irreducible. By Proposition 3.2.9, $SA_{2^{s-j+2}}$ is $(s-j)$-extraspecial. Hence by Theorem 3.2.8, $\langle ad^{2^j}, N\rangle$ and $\langle a, D\rangle$ are conjugate in $GL(2, \mathbb{F})$. ■

By combining all of the results we have thus far, we get the following theorem.

**3.4.14 Theorem.** *For odd $p$, the following subgroups of $M$ form a complete and irredundant set of $GL(2, \mathbb{F})$-conjugacy class representatives of the 2-subgroups of $M$ not contained in $B$:*

$$\begin{aligned}
&\langle a\rangle\,;\\
&\langle a, T\rangle\,;\\
&\langle a, N\rangle\,, \quad N \trianglelefteq M,\ U\cap V \leq N \leq UV\,;\\
&\langle ad^{2^j}, N\rangle\,, \quad N \trianglelefteq M,\ U\cap V \leq N \leq UV,\ N\cap V = V^{2^j}\,;\\
&\langle a, D\rangle\,, \quad D \trianglelefteq M,\ U\cap V \leq D \leq UV,\ D \geq U^{2^{s-2}}\,.
\end{aligned}$$

*In this list $D$ and $N$ stand for diagonal and non-diagonal subgroups, respectively.* ■

We have avoided repetition of $GL(2, \mathbb{F})$-conjugacy classes by placing the stated restriction on $D$. Alternatively, we could have placed some restrictions on $N$.

## 3.5 The irreducible subgroups of $M$

If $\{q_1, \ldots, q_r\}$ is the set of odd primes that divide $p^k - 1$, then a complete and irredundant set of $GL(2, \mathbb{F})$-conjugacy class representatives of the subgroups of $M$ not contained in $B$ is

$$\mathcal{S} := \{\langle G, P_1, \ldots, P_r\rangle\}\,,$$

where $G$ runs through the members of the list of 2-subgroups in Theorem 3.4.14, and each $P_i$ runs through the list of normal $q_i$-subgroups of $M$, as described in Theorem 3.3.1.

All that remains to do is to eliminate the reducible groups from $\mathcal{S}$. Every irreducible abelian linear group is cyclic, and every irreducible cyclic subgroup of $GL(2,\mathbb{F})$ is conjugate to a subgroup of our fixed Singer cycle; we deal with those subgroups in the next chapter, and so can ignore them here. Recognising the abelian subgroups of $M$ is easy, as the next proposition shows.

**3.5.1 Proposition.** *A subgroup of $M$ not contained in $B$ is abelian if and only if its intersection with $B$ is a subgroup of $\langle bc \rangle$.*

**Proof.** Let $G$ be an abelian subgroup of $M$ not contained in $B$. Choose an element $ab^m c^n$ of $M$ not in $B$. This element acts trivially on every element of $G \cap B$, and therefore $a$ also acts trivially on every element of $G \cap B$. It is easy to check that $\mathbf{C}_M(a) = \langle bc \rangle$; therefore $G \cap B \leq \langle bc \rangle$.

Conversely, let $H$ be a subgroup of $M$ not contained in $B$ whose intersection with $B$ is a subgroup of $\langle bc \rangle$. Since $\langle bc \rangle$ is central in $M$, and the central quotient of a group cannot have prime order, it follows that $H$ is abelian. ■

If $p$ is odd, then every non-abelian subgroup of $M$ is completely reducible by Maschke's Theorem, and since we are in degree 2, the completely reducible non-abelian subgroups are irreducible.

Finally, we have our desired list of groups:

**3.5.2 Theorem.** *For odd $p$, the following is a complete and irredundant set of $GL(2,\mathbb{F})$-conjugacy class representatives of the non-abelian imprimitive soluble subgroups of $GL(2,\mathbb{F})$:*

$$\{\langle G, P_1, \ldots, P_r \rangle\},$$

*where $G$ runs through the members of the list of 2-subgroups in Theorem 3.4.14, and each $P_i$ runs through the list of normal $q_i$-subgroups of $M$, as described by Theorem 3.3.1, and $G \cap B \not\leq \langle d_2 e_2 \rangle$ and/or at least one $P_i \not\leq \langle d_{q_i} e_{q_i} \rangle$.* ■

# Chapter 4

# The primitive subgroups of the normaliser of the Singer cycle of prime degree

Let $q$ be a prime, and let $\mathbb{F}$ be the field of $p^k$ elements. Let $A$ be our fixed Singer cycle of $GL(q, \mathbb{F})$, and let $M$ be its normaliser. A polycyclic presentation for $M$ is

$$\langle a, b \mid a^q = 1, \quad b^a = b^{p^k}, \quad b^{p^{kq}-1} = 1 \rangle,$$

where the matrices $a$ and $b$ are as defined in Section 2.3. In this chapter we give a theorem that provides a complete and irredundant list of $GL(q, \mathbb{F})$-conjugacy class representatives of the primitive subgroups and the imprimitive cyclic subgroups of $M$. First we give some preliminary lemmas.

**4.1.1 Lemma.** *(a) If* $q \nmid (p^k - 1)$, *then* $q \nmid (p^{kq} - 1)$.
*(b) If* $q \mid (p^k - 1)$, *then* $q \| (p^{kq} - 1)/(p^k - 1)$, *except when* $q = 2$ *and* $p^k \equiv 3 \bmod 4$.

**Proof.** (a) If $q = p$, then the statement is trivial, so suppose that $q \neq p$. Then by Fermat's Little Theorem, $p^{kq} \equiv p^k \bmod q$. The statement then follows by observing that $p^{kq} - 1 = (p^{kq} - p^k) + (p^k - 1)$.
(b) If $q = 2$ and $p^k \equiv 1 \bmod 4$, then $q \| (p^k + 1)$, as required. Suppose that $q > 2$,

and write $p^k = 1 + lq$, for some positive integer $l$. Then

$$\begin{aligned}
\tfrac{p^{kq}-1}{p^k-1} &= 1 + (1+lq) + (1+lq)^2 + \ldots + (1+lq)^{q-1} \\
&= (1 + 1 + \ldots + 1) + (lq + 2lq + \ldots + (q-1)lq) + nq^2, \text{ for some } n \\
&= q + lq^2(q-1)/2 + nq^2 \\
&\equiv q \bmod q^2,
\end{aligned}$$

thus proving the second statement. ■

**4.1.2 Lemma.** *(a)* $(a^i b^j)^m = a^{im} b^{j(p^{km}-1)/(p^{ki}-1)}$ *(i and m positive).*
*(b)* $(a^i b^j)^{a^r b^s} = a^i b^{jp^{kr} - s(p^{ki}-1)}$ *(i and r positive).* ■

**4.1.3 Lemma.** *For all integers n, u and v, there exists an integer w such that*

$$(ab^n)^{a^u b^v} = (ab^n)^{b^w}.$$

**Proof.** It can be checked that setting $w = v - n(p^{ku} - 1)/(p^k - 1)$ makes the above equation true. ■

Now we organise the subgroups of $M$ into conjugacy classes. Since $A$ is a cyclic normal subgroup of $M$, it follows that each of its subgroups is normal in $M$.

**4.1.4 Lemma.** *If $G \leq M$, then $G$ is conjugate in $M$ to $\langle a, G \cap A \rangle$ if and only if $G$ contains an element of the form $ab^{n(p^k-1)}$, for some integer $n$.*

**Proof.** Suppose that $G$ conjugated by $a^i b^j$ equals $\langle a, G \cap A \rangle$. Then $G$ contains $a^{b^{-j}a^{-i}}$, which equals $ab^{jp^k(q-i)(p^k-1)}$, as required.

Conversely, suppose that $G$ contains $ab^{n(p^k-1)}$. Then $G^{b^n}$ contains $a$. ■

**4.1.5 Lemma.** *If $G \leq M$ and $G$ splits over $G \cap A$, then $G$ is conjugate in $M$ to $\langle a, G \cap A \rangle$.*

**Proof.** Suppose that $G = \langle a^r b^s, G \cap A \rangle$, where $a^r b^s$ has order $q$. By raising $a^r b^s$ to the inverse of $r$ modulo $q$, we can reduce the exponent on $a$ to 1. Therefore, without loss of generality, we can assume that $r = 1$. By hypothesis, $(ab^s)^q = 1$. Since $(ab^s)^q$ equals $b$ raised to the power of $s(p^{kq} - 1)/(p^k - 1)$, it follows that $(p^k - 1) \mid s$. The result then follows from Lemma 4.1.4. ■

The subgroups of $A$ are easy to list, so let us now concentrate on the subgroups of $M$ not contained in $A$. Let $G$ be a subgroup of $M$ not contained in $A$, and set $B := G \cap A$. As remarked earlier, $B \trianglelefteq M$. Since $|G/B| = q$, we can choose a $q$-element $ab^m \in G$ such that $G = \langle ab^m, B \rangle$. Since $(ab^m)^q$ equals $b$ raised to the power of $m(p^{kq}-1)/(p^k-1)$, we see that $(ab^m)^q$ is scalar. Denote the scalar group by $S$. We have that $\langle (ab^m)^q \rangle \leq O_q(B \cap S)$. If $\langle (ab^m)^q \rangle < O_q(B \cap S)$, then there is an element of $B$ which centralises $ab^m$ and whose $q$-th power equals $(ab^m)^q$. Then by Lemmas 3.2.6 and 4.1.5, $G$ is conjugate in $M$ to $\langle a, B \rangle$. Now assume that $(ab^m)^q$ generates $O_q(B \cap S)$, say

$$\langle (ab^m)^q \rangle = \langle b^{(p^{kq}-1)/q^i} \rangle ,$$

where $i$ is some integer such that $q^i \,|\, (p^{kq}-1)$. If $q \nmid (p^k-1)$, then by Lemma 4.1.1a $i = 0$ and $ab^m$ has order $q$. If $ab^m$ has order $q$, then by Lemma 4.1.5, $G$ is conjugate in $M$ to $\langle a, B \rangle$. So let us assume that $q \,|\, (p^k-1)$ and that $(ab^m)^q \neq 1$. Write $p^k - 1 = q^\alpha l$, where $q \nmid l$; then by our assumptions so far we have that $1 \leq i \leq \alpha$. We now establish a 'normal form' for a representative of the conjugacy class containing $G$.

**4.1.6 Lemma.** *$G$ is conjugate in $M$ to $\langle ab^{q^{\alpha-i}lr}, B \rangle$, where $1 \leq r \leq q-1$.*

**Proof.** Write $m$ as $q^j n$, where $q \nmid n$. Since $\langle (ab^m)^q \rangle = \langle b^{(p^{kq}-1)/q^i} \rangle$, it follows that $j = \alpha - i$ and that $l \,|\, n$. Now set $s := n/l$, and let $r$ be the integer between 1 and $q-1$ such that $s \equiv r \bmod q$. Let $t$ be the largest divisor of $(p^{kq}-1)/(p^k-1)$ that is prime to $q^{i-1}$, and choose $u$ and $v$ so that $q^{i-1}u = 1 + vt$. Finally, set $w := v(s-r)/q$. Then

$$G = \langle (ab^m) b^{w(p^{kq}-1)/q^i}, B \rangle .$$

Let us simplify the exponent on $b$ in the first element of this generating set. If $q$ is odd or $p^k \equiv 1 \bmod 4$, or both, then $q^{\alpha+1} \| (p^{kq}-1)$ by Lemma 4.1.1b. Then

$$\begin{aligned} m + w(p^{kq}-1)/q^i &= q^{\alpha-i}ls + v(s-r)q^{\alpha+1}lt/q^{i+1} \\ &= q^{\alpha-i}l(s + v(s-r)t) \\ &= q^{\alpha-i}l(s + (vt+1)(s-r) - (s-r)) \\ &= q^{\alpha-i}l(r + q^{i-1}u(s-r)) \\ &= q^{\alpha-i}lr + q^{\alpha-1}lu(s-r) \\ &= q^{\alpha-i}lr + u(s-r)(p^k-1)/q\,. \end{aligned}$$

If $q = 2$ and $p^k \equiv 3 \bmod 4$, then $\alpha = i = r = u = 1$, and $v = w = 0$, so

$$\begin{aligned} m + w(p^{kq}-1)/q^i &= m \\ &= q^{\alpha-i}ls \\ &= ls \\ &= l + (s-1)l \\ &= q^{\alpha-i}lr + u(s-r)(p^k-1)/q\,. \end{aligned}$$

So we see that if we conjugate the first element of this generating set by $b^{u(s-r)/q}$, then we get $ab^{q^{\alpha-i}lr}$, as required. ∎

**4.1.7 Lemma.** *Let $B$ be as above, and let $1 \le r < s \le q-1$. Denote $\langle ab^{q^{\alpha-i}lr}, B\rangle$ by $G_1$, and denote $\langle ab^{q^{\alpha-i}ls}, B\rangle$ by $G_2$. Then $G_1$ is not conjugate in $M$ to $G_2$.*

**Proof.** Note that $q$ must be odd to satisfy the hypotheses of the lemma, and so $q^{\alpha+1} \| (p^{kq}-1)$, by Lemma 4.1.1b. Suppose that $G_1$ and $G_2$ are conjugate in $M$. Then there is an integer $u$ and an element $b^v$ (by Lemmas 4.1.2b and 4.1.3) such that $ab^{q^{\alpha-i}lr}b^{u(p^{kq}-1)/q^i}$ conjugated by $b^v$ equals $ab^{q^{\alpha-i}ls}$. Therefore

$$q^{\alpha-i}lr + u(p^{kq}-1)/q^i - v(p^k-1) \equiv q^{\alpha-i}ls \bmod (p^{kq}-1)\,.$$

In particular, $q^{\alpha+1}$ divides

$$q^{\alpha-i}lr + u(p^{kq}-1)/q^i - v(p^k-1) - q^{\alpha-i}ls\,,$$

which equals

$$q^{\alpha-i}l(r-s) + uq^{\alpha+1-i}lt - vq^{\alpha}l\,,$$

where $t$ is the largest divisor of $(p^{kq}-1)/(p^k-1)$ prime to $q$. Therefore $q^{i+1}$ divides

$$l(r-s)+uqlt-vq^il\,,$$

which implies that $q|(r-s)$, a contradiction. Hence $G_1$ is not conjugate in $M$ to $G_2$. ■

**4.1.8 Lemma.** *Let $B$ be as above. Denote $\langle a,B\rangle$ by $G_1$, and denote $\langle ab^{q^{\alpha-i}lr},B\rangle$ by $G_2$, where $1\le r\le q-1$. Then $G_1$ is not conjugate in $GL(q,\mathbb{F})$ to $G_2$, except when $B$ contains the Sylow $q$-subgroup of $A$, in which case $G_1$ and $G_2$ are conjugate in $M$.*

**Proof.** Suppose that $B$ contains the Sylow $q$-subgroup of $A$. Then each of $G_1$ and $G_2$ contain a Sylow $q$-subgroup of $M$. These two Sylow $q$-subgroups are conjugate in $M$, and clearly, any element that conjugates the second to the first will also conjugate $G_2$ to $G_1$.

Suppose that $B$ does not contain the Sylow $q$-subgroup of $A$. Consider the subgroups $\langle a,b^{(p^{kq}-1)/q^i}\rangle$ of $G_1$, and $\langle ab^{q^{\alpha-i}lr},b^{(p^{kq}-1)/q^i}\rangle$ of $G_2$. The first of these is abelian but not cyclic, while the second is cyclic. If $q$ is odd or $p^k\equiv 1 \bmod 4$, or both, then these subgroups are Sylow $q$-subgroups of $G_1$ and $G_2$, respectively; therefore $G_1$ and $G_2$ are not isomorphic, and so cannot be conjugate in $GL(q,\mathbb{F})$. Now suppose that $q=2$ and that $p^k\equiv 3 \bmod 4$ (so $\alpha=i=r=1$). Then it is not difficult to show that $G_2$ contains a unique element of order 2, whereas $G_1$ clearly contains at least two such elements. Again, $G_1\ncong G_2$, and so the two groups cannot be conjugate in $GL(2,\mathbb{F})$. ■

By combining all of the lemmas so far we get the following theorem.

**4.1.9 Theorem.** *The following groups form a complete and irredundant set of $M$-conjugacy class representatives of the subgroups of $M$:*

$$\begin{aligned}
&\langle B\rangle\,, && B\le A;\\
&\langle a,C\rangle\,, && C\le A;\\
&\langle ab^{q^{\alpha-i}lr},D\rangle\,, && D\le A,\quad O_q(A)\not\le D,\\
& && O_q(D\cap S)=\langle b^{(p^{kq}-1)/q^i}\rangle\,, i\ne 0\,, r=1,\dots,q-1\,. \blacksquare
\end{aligned}$$

Now we must select from this list the primitive groups and imprimitive cyclic groups. By Theorem 2.3.3, every cyclic irreducible subgroup of $M$ is $GL(q, \mathbb{F})$-conjugate to a subgroup of $A$.

**4.1.10 Proposition.** *An irreducible subgroup of $A$ is imprimitive if and only if its order divides $q(p^k - 1)$ but does not divide $p^k - 1$.*

**Proof.** Let $x \in A$, and suppose that the subgroup $C$ generated by $x$ is imprimitive. Since $C$ is irreducible, its order cannot divide $p^k - 1$, and since the degree is prime, the natural module for $C$ must decompose into a direct sum of $q$ 1-dimensional subspaces, permuted transitively by $x$. An abelian transitive permutation group of degree $q$ must have order $q$, and hence $x^q$ stabilises this system of imprimitivity for $C$. Therefore $x^q$ generates a proper subgroup $D$ of $C$, of index $q$. By construction, the natural module for $D$ decomposes into a direct sum of $q$ 1-dimensional submodules. Therefore $D$ is (conjugate to) a subgroup of the diagonal group and so its exponent divides $p^k - 1$. Since $D$ is cyclic, it follows that its order also divides $p^k - 1$. So the order of $C$ divides $q(p^k - 1)$.

Conversely, suppose that the order of the irreducible subgroup $C$ generated by $x$ divides $q(p^k - 1)$ but does not divide $p^k - 1$. Since $|C^q|$ divides $p^k - 1$, it follows that $C^q$ is reducible (see Theorem 2.3.2). Since $C$ is irreducible, $C^q$ is completely reducible. By Clifford's Theorem, if $U$ is the natural module for $C$, then there is a 1-dimensional subspace $V$ of $U$ which admits $C^q$. Then it is easy to show that

$$U = V \oplus Vx \oplus \ldots \oplus Vx^{q-1},$$

from which it is obvious that $C$ is imprimitive. ∎

**4.1.11 Proposition.** *A subgroup of $A$ is irreducible if and only if its order does not divide $p^k - 1$.*

**Proof.** Let $B$ be an irreducible subgroup of $A$. Since the subgroup of $A$ of order $p^k - 1$ is the scalar group, $|B|$ cannot divide $p^k - 1$.

Conversely, let $B$ be a subgroup of $A$ of order not dividing $p^k - 1$. Note that $A$ is primitive by the above proposition. Then by Clifford's Theorem, the natural

module for $B$ is completely reducible and homogeneous. If this module were reducible, then $B$ would be scalar (because the degree is prime), a contradiction. Therefore $B$ is irreducible. ■

Now we consider the primitive non-abelian subgroups of $M$.

**4.1.12 Proposition.** *A subgroup $G$ of $M$ not contained in $A$ is abelian if and only if $|G \cap A|$ divides $p^k - 1$.*

**Proof.** If $G \cap A = \langle b^n \rangle$, where $n \mid (p^{kq} - 1)$, then $G$ is abelian if and only if $(b^n)^a = b^n$. Therefore $G \cap A$ must be a subgroup of the scalar group. ■

**4.1.13 Proposition.** *Let $G$ equal $\langle a, B \rangle$, where $B = G \cap A$, and suppose that $G$ is non-abelian. Then $G$ is primitive if and only if $B$ is primitive.*

**Proof.** If $B$ is primitive, then of course $G$ is primitive. Suppose that $B = \langle b^n \rangle$ and is not primitive. Clearly $B$ cannot be reducible, for then $G$ would be abelian, by the last two propositions. Hence $B$ is imprimitive. Then $B^q$ is a proper subgroup of $B$, and scalar. In particular, $q \mid (p^{kq} - 1)$ and therefore $q \mid (p^k - 1)$, by Lemma 4.1.1a. Hence $\langle a \rangle$ is reducible by Theorem 2.3.2, and completely reducible by Maschke's Theorem. Therefore the natural module for $\langle a \rangle$ is the direct sum of $q$ 1-dimensional submodules. Let $V$ be any one of these direct summands, and let $U$ be the natural module for $G$. Since $G$ is irreducible, it is easy to show that $U$ has the vector space decomposition

$$U = V \oplus Vb^n \oplus \ldots \oplus Vb^{n(q-1)}.$$

This yields a system of imprimitivity for $B$, because $b^{nq}$ is scalar. Furthermore, for each integer $i$ such that $0 \leq i \leq q - 1$, we have

$$\begin{aligned} Vb^{ni}a &= Vaa^{-1}b^{ni}a \\ &= Vb^{nip^k} \\ &= Vb^{ni(p^k-1)}b^{ni} \\ &= Vb^{ni}, \end{aligned}$$

because $q \mid (p^k - 1)$ and $b^{nq}$ is scalar. Therefore the above decomposition of $U$ yields a system of imprimitivity for $G$. Hence if $G$ is primitive, then so is $B$. ■

**4.1.14 Proposition.** *Suppose that* $q|(p^k-1)$, *and let* $p^k-1=q^\alpha l$, *where* $q\nmid l$. *Let* $B$ *be a subgroup of* $A$ *such that the Sylow* $q$*-subgroup of the intersection of* $B$ *and the scalar group is generated by* $b^{(p^{kq}-1)/q^i}$, *where* $i\neq 0$. *Let* $1\leq r\leq q-1$, *and set* $G:=\langle ab^{q^{\alpha-i}lr},B\rangle$. *If* $G$ *is non-abelian, then* $G$ *is primitive.*

**Proof.** If $G$ were reducible, then $B$ would be reducible and so scalar, making $G$ abelian. So $G$ is irreducible. Suppose that $G$ is imprimitive. Again, $B$ cannot be reducible, so is imprimitive, and therefore $B^q$ is a proper subgroup of $B$, and scalar. Since $G$ is non-abelian, $Z(G)=B^q$. Since $|G/B^q|=q^2$, we have that $G'$ is central, and so $G$ is nilpotent. The Sylow subgroups of $G$ corresponding to primes other than $q$ lie in $B^q$ and so are cyclic. If $q$ is odd or $p^k\equiv 1 \bmod 4$, or both, then we see from the proof of Lemma 4.1.8 that the Sylow $q$-subgroups of $G$ are also cyclic. Then $G$ would be abelian, a contradiction. So $q=2$ and $p^k\equiv 3 \bmod 4$. Also from the proof of Lemma 4.1.8, the Sylow 2-subgroups of $G$ have a unique element of order 2. Therefore they are either cyclic or generalised quaternion (see Suzuki (1986, 4.4, p. 59)). If they were cyclic, then $G$ would be abelian. So the Sylow 2-subgroups of $G$ are generalised quaternion, and imprimitive. But from Chapter 3, we know that the imprimitive 2-subgroups of $GL(2,p^k)$ when $p^k\equiv 3 \bmod 4$ are subgroups of $C_2 \operatorname{wr} C_2$, which is isomorphic to $D_8$. This is another contradiction. Hence $G$ is primitive. ∎

**4.1.15 Proposition.** *Suppose that* $q|(p^k-1)$, *and let* $p^k-1=q^\alpha l$, *where* $q\nmid l$. *Let* $B$ *be a subgroup of* $A$ *such that the Sylow* $q$*-subgroup of the intersection of* $B$ *and the scalar group is generated by* $b^{(p^{kq}-1)/q^i}$, *where* $i\neq 0$. *Let* $1\leq r<s\leq q-1$, *set* $G_1:=\langle ab^{q^{\alpha-i}lr},B\rangle$, *and set* $G_2:=\langle ab^{q^{\alpha-i}ls},B\rangle$. *Then* $G_1$ *is abelian if and only if* $G_2$ *is abelian. If* $G_1$ *is not abelian, then* $G_1$ *is not conjugate in* $GL(q,\mathbb{F})$ *to* $G_2$.

**Proof.** It is clear that $G_1$ is abelian if and only if $B$ is scalar if and only if $G_2$ is abelian. Suppose that $G_1$ is not abelian. Since $r$ and $s$ are unequal, $q$ must be odd. Therefore all the Sylow subgroups of $G_1$ are cyclic. If $G_1$ were nilpotent, then it would be abelian, a contradiction. Hence $G_1$ is not nilpotent, and so its Fitting subgroup is $B$. The same argument applies to $G_2$. Suppose that $G_1$ and $G_2$ are conjugate in $GL(q,\mathbb{F})$, say $G_1^x=G_2$. Then $x$ normalises $B$. Since

$G_1$ is non-abelian, $|B|$ cannot divide $p^k - 1$. Therefore (see Theorem 2.3.5) the normaliser in $GL(q, \mathbb{F})$ of $B$ is $M$. So $x \in M$, a contradiction, because $G_1$ and $G_2$ are not conjugate in $M$, by Lemma 4.1.7. ∎

By combining all of the results of this chapter we get the following theorem.

**4.1.16 Theorem.** *The following groups form a complete and irredundant set of $GL(q, \mathbb{F})$-conjugacy class representatives of the primitive subgroups and cyclic imprimitive subgroups of $M$:*

$$\begin{aligned}
&\langle B \rangle, && B \leq A, \quad |B| \nmid (p^k - 1);\\
&\langle a, C \rangle, && C \leq A, \quad |C| \nmid q(p^k - 1);\\
&\langle ab^{q^{\alpha-i}lr}, D \rangle, && D \leq A, \quad O_q(A) \not\leq D, \quad |D| \nmid (p^k - 1),\\
& && O_q(D \cap S) = \langle b^{(p^{kq}-1)/q^i} \rangle, i \neq 0, r = 1, \ldots, q-1. \blacksquare
\end{aligned}$$

# Chapter 5

# The irreducible soluble subgroups of $GL(2, p^k)$

Let $\mathbb{F}$ be the field of $p^k$ elements. Since $GL(1, \mathbb{F})$ and $S_2$ are soluble, there is exactly one JS-imprimitive of $GL(2, \mathbb{F})$, namely

$$M_1 := GL(1, \mathbb{F}) \operatorname{wr} S_2 \quad (p^k \neq 2).$$

Theorem 3.5.2 provides a complete and irredundant list $\mathcal{L}_1$ of $GL(2, \mathbb{F})$-conjugacy class representatives of the non-cyclic irreducible subgroups of $M_1$.

Now consider the JS-primitives of $GL(2, \mathbb{F})$. The unique maximal abelian normal subgroup of such a group has order either $p^{2k} - 1$ or $p^k - 1$. There is just one JS-primitive of the first kind, namely

$$M_2 := C_{p^{2k}-1} \rtimes C_2 \,,$$

the normaliser of a Singer cycle. Theorem 4.1.16 provides a complete and irredundant list $\mathcal{L}_2$ of $GL(2, \mathbb{F})$-conjugacy class representatives of the primitive subgroups and imprimitive cyclic subgroups of $M_2$.

There are JS-primitives whose unique maximal abelian normal subgroup has order $p^k - 1$ if and only if $p$ is odd. By Remark 2.5.36, they can be written as

$$\begin{aligned} M_3 &:= (C_{p^k-1} \circ Q_8) \rtimes O^-(2,2)\,, \quad p^k \equiv 3 \bmod 4\,, \\ M_4 &:= (C_{p^k-1} \circ Q_8) \rtimes Sp(2,2)\,, \quad p^k \equiv 1 \bmod 4\,. \end{aligned}$$

In this chapter we give theorems which provide complete and irredundant lists $\mathcal{L}_i$, $i = 3, 4$, of $GL(2, \mathbb{F})$-conjugacy class representatives of the primitive soluble

subgroups of $GL(2,\mathbb{F})$ whose guardian is $M_i$. Then the combination of $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_i$ gives us a complete and irredundant list of $GL(2,\mathbb{F})$-conjugacy class representatives of the irreducible soluble subgroups of $GL(2,\mathbb{F})$.

We mention in passing which of the above JS-maximals are maximal soluble subgroups of $GL(2,\mathbb{F})$. Both Jordan (1871a, Table A, p. 288) and Suprunenko (1976, footnote on p. 165) knew the following result; it is easily proved using elementary number theory and some basic structural properties of the groups concerned.

**5.0.1 Proposition.** *(a) $M_1$ is a maximal soluble subgroup of $GL(2,\mathbb{F})$ except when $p^k = 3$ (in which case $M_1$ is conjugate to subgroups of both $M_2$ and $M_3$) and when $p^k = 5$ (in which case $M_1$ is conjugate to a subgroup of $M_4$).*

*(b) $M_2$ is a maximal soluble subgroup of $GL(2,\mathbb{F})$ except when $p^k = 3$ (in which case $M_2$ is a subgroup of $M_3$).*

*(c) $M_3$ is a maximal soluble subgroup of $GL(2,\mathbb{F})$.*

*(d) $M_4$ is a maximal soluble subgroup of $GL(2,\mathbb{F})$.* ∎

## 5.1 Miscellaneous results

**5.1.1 Proposition.** *Let $V$ be a vector space, and let $A$ be the scalar subgroup of $GL(V)$. Let $G$ be a subgroup of $GL(V)$ containing $A$, and suppose that $G = NA$ for some subgroup $N$ of $G$. Let $H$ be a subgroup of $G$ containing $N \cap A$. Then*

*(a) $H$ is irreducible if and only if $N \cap HA$ is irreducible;*

*(b) $H$ is primitive if and only if $N \cap HA$ is primitive.*

**Proof.** By Dedekind's Modular Law we have that $HA = (N \cap HA)A$. Since multiplication by scalars does not affect the reducibility or primitivity of a group, the result now follows. ∎

**5.1.2 Definition.** The *Burnside lattice*, $\mathcal{L}$, of a group $G$ is a lattice with the following properties.

(i) Each element of $\mathcal{L}$ represents a conjugacy class of subgroups of $G$, and each

conjugacy class is represented exactly once in $\mathcal{L}$.

(ii) If $C$ and $D$ are elements of $\mathcal{L}$, then we write $C \leq D$ if and only if at least one group in the conjugacy class represented by $C$ is a subgroup of at least one group in the conjugacy class represented by $D$.

**5.1.3 Notation.** We draw the Burnside lattice $\mathcal{L}$ of a group $G$ according to the following rules.

(i) We represent elements of $\mathcal{L}$ by small black discs.

(ii) If an element of $\mathcal{L}$ represents a conjugacy class containing a single group (which is therefore normal in $G$), we draw a circle around the disc representing that element.

(iii) We label each disc with either the isomorphism type or the order of the groups in the conjugacy class it represents.

(iv) We represent the relation $C \leq D$ by placing the disc representing $C$ lower on the page than the disc representing $D$ and by drawing a line between those two discs. However, we suppress inclusions that are implied by the reflexiveness and transitivity of $\leq$.

**5.1.4 Definition.** Let $m \geq 2$ and $n \geq 3$. We will denote by $I_n^{2m}$ (the $I$ standing for 'inversion') any group isomorphic to the following soluble group of order $2mn$:

$$\begin{aligned} \langle a, b \mid\ & a^{2m} = 1, \\ & b^a = b^{-1},\ \ b^n = 1 \rangle . \end{aligned}$$

**5.1.5 Definition.** We will denote by $SL(2,3)$ any group isomorphic to the following soluble group of order 24:

$$\begin{aligned} \langle a, b, c \mid\ & a^3 = 1, \\ & b^a = c,\ \ b^2 = c^2, \\ & c^a = bc,\ \ c^b = c^3,\ \ c^4 = 1 \rangle . \end{aligned}$$

**5.1.6 Definition.** We will denote by $GL(2,3)$ any group isomorphic to the fol-

lowing soluble group of order 48:

$$\begin{aligned}\langle a, b, c, d \mid\ & a^2 = 1, \\ & b^a = b^2, \quad b^3 = 1, \\ & c^a = d^3, \quad c^b = d, \quad c^2 = d^2, \\ & d^a = cd^2, \quad d^b = cd, \quad d^c = d^3, \quad d^4 = 1 \rangle .\end{aligned}$$

The Burnside lattice of $GL(2,3)$ is pictured in Figure 5.1. This can be checked via CAYLEY, or in the tables of Neubüser (1967) where $GL(2,3)$ has the number 48.49.

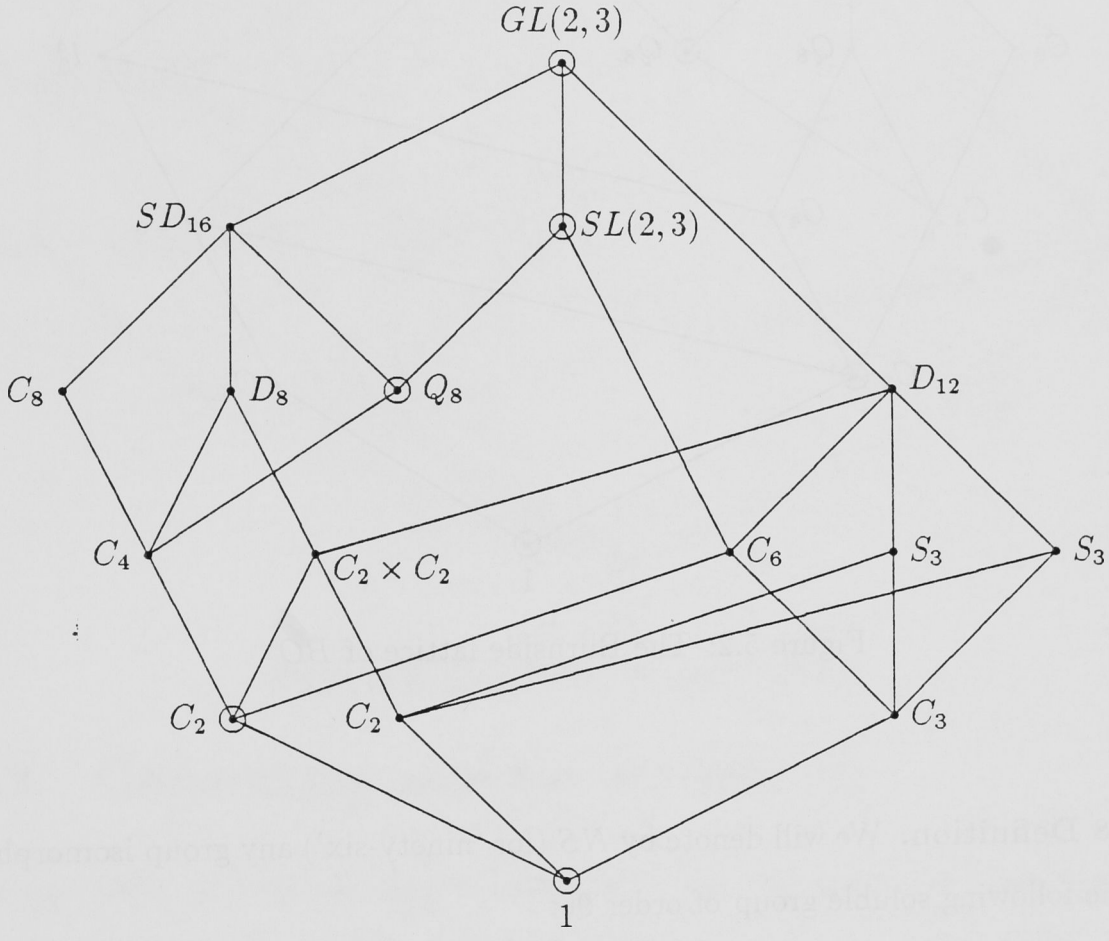



Figure 5.1: The Burnside lattice of $GL(2,3)$

**5.1.7 Definition.** We will denote by $BO$ (for *binary octahedral*) any group isomorphic to the following soluble group of order 48:

$$\begin{aligned}\langle a, b, c, d \mid\ & a^2 = d^2, \\ & b^a = b^2, \quad b^3 = 1, \\ & c^a = d^3, \quad c^b = d, \quad c^2 = d^2, \\ & d^a = cd^2, \quad d^b = cd, \quad d^c = d^3, \quad d^4 = 1 \rangle .\end{aligned}$$

The Burnside lattice of $BO$ is pictured in Figure 5.2. This can be checked via CAYLEY, or in the tables of Neubüser (1967) where $BO$ has the number 48.50.

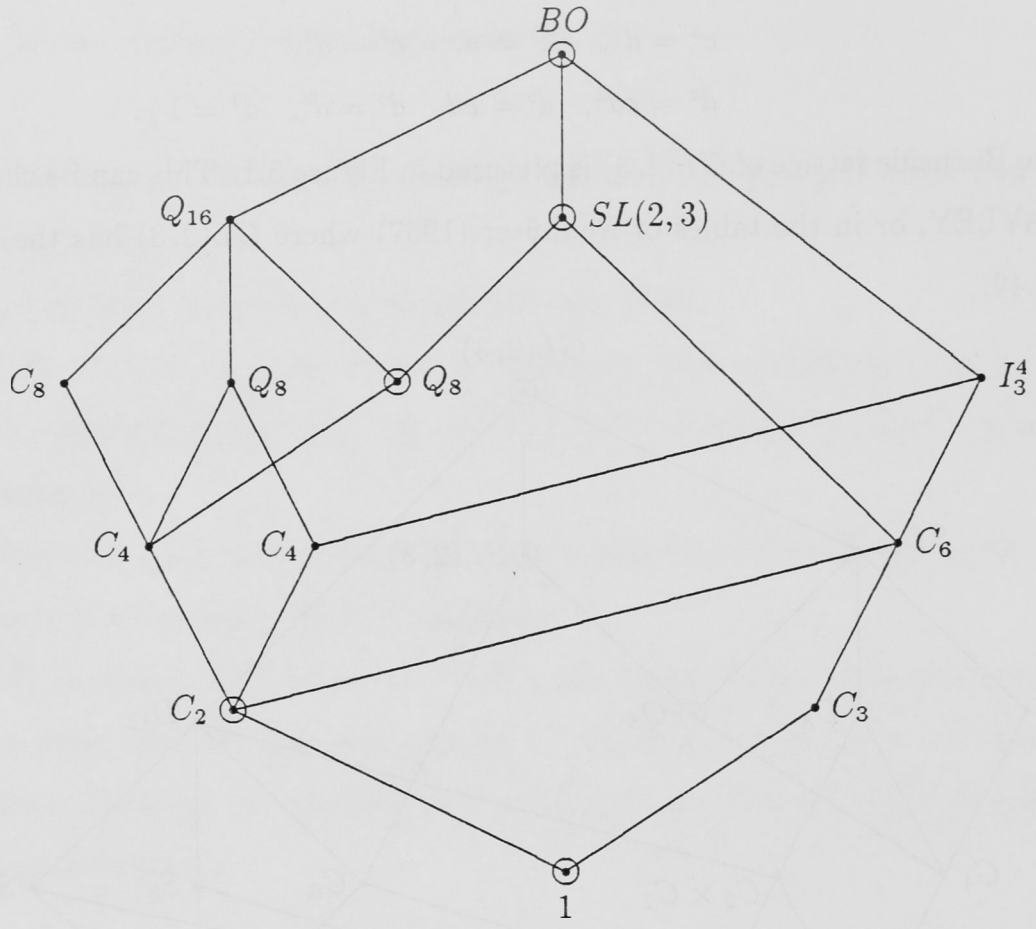



Figure 5.2: The Burnside lattice of $BO$

**5.1.8 Definition.** We will denote by $NS$ (for 'ninety-six') any group isomorphic to the following soluble group of order 96:

$$\begin{aligned}\langle a,b,c,d,e \mid\ & a^2=e,\\ & b^a=b^2, \quad b^3=1,\\ & c^a=de^2, \quad c^b=d, \quad c^2=e^2,\\ & d^a=ce^2, \quad d^b=cd, \quad d^c=de^2, \quad d^2=e^2,\\ & e^a=e, \quad e^b=e, \quad e^c=e, \quad e^d=e, \quad e^4=1\rangle.\end{aligned}$$

The Burnside lattice of $NS$ is pictured in Figure 5.3. This can be checked via CAYLEY.

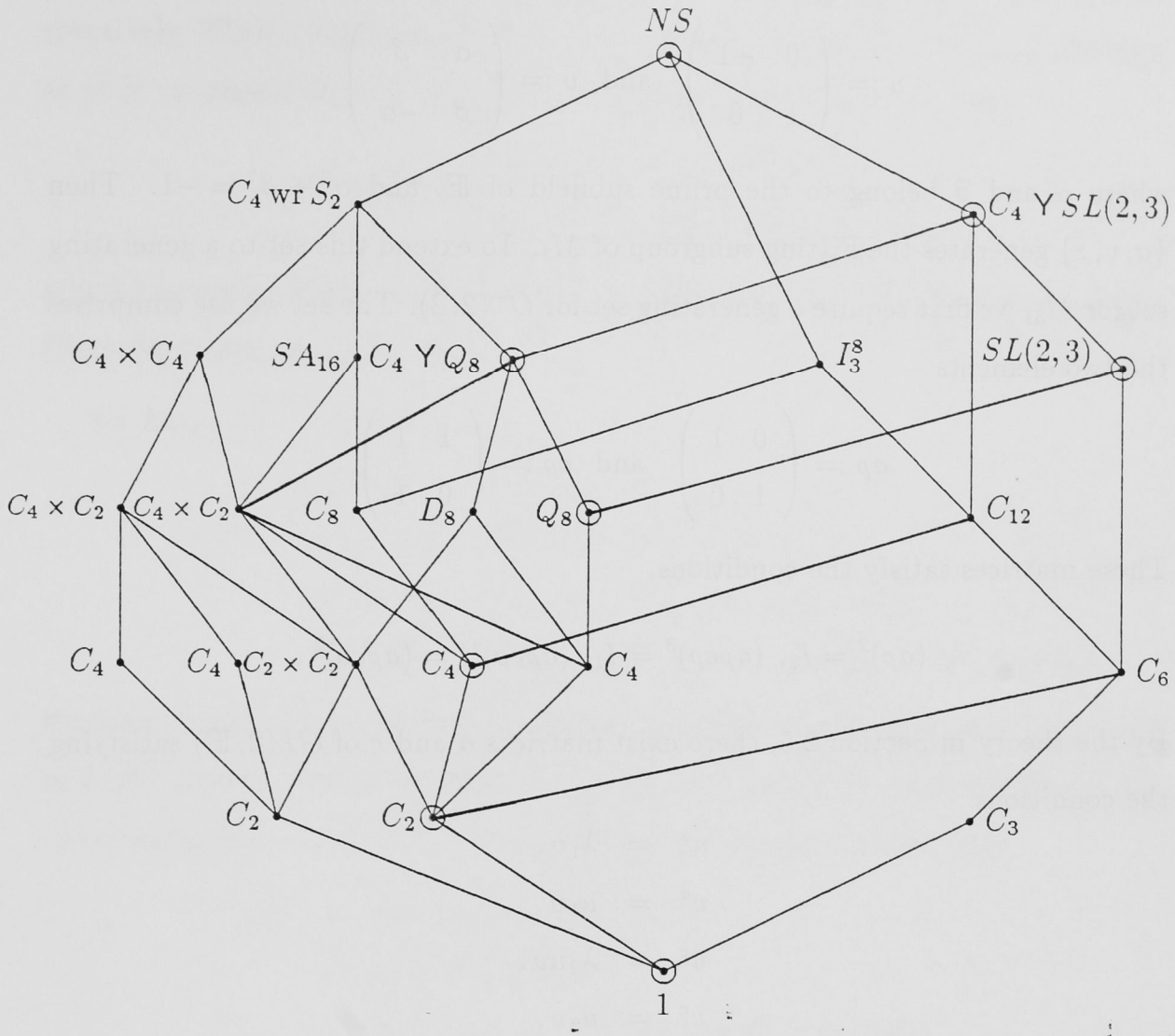



Figure 5.3: The Burnside lattice of $NS$

## 5.2 Generating sets for $M_3$ and $M_4$

Jordan (1868, p. 112) and Suprunenko (1976, pp. 162-164) have already each given generating sets for $M_3$ and $M_4$, but they do not give corresponding sets of defining relations. In this section we derive polycyclic presentations for $M_3$ and $M_4$. We will find that in both of these groups the scalar group has a proper supplement. This does not seem to have been noted before.

### 5.2.1 A generating set for $M_3$

Recall that $M_3$ is only defined when $p^k \equiv 3 \bmod 4$. We construct a generating set for $M_3$ by the methods described in Section 2.5. Let $z$ be a generator for the

scalar group, and define $u$ and $v$ by

$$u := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad v := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix},$$

where $\alpha$ and $\beta$ belong to the prime subfield of $\mathbb{F}$, and $\alpha^2 + \beta^2 = -1$. Then $\{u, v, z\}$ generates the Fitting subgroup of $M_3$. To extend this set to a generating set for $M_3$, we first require a generating set for $O^-(2,2)$. The set we use comprises the two elements

$$a\rho := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad c\rho := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

These matrices satisfy the conditions

$$(a\rho)^2 = I_2,\ (a\rho c\rho)^3 = I_2,\ (a\rho c\rho)^{a\rho} = (a\rho c\rho)^2.$$

By the theory in Section 2.5, there exist matrices $a$ and $c$ of $GL(2,\mathbb{F})$ satisfying the conditions

$$\begin{aligned} u^a &= \lambda_1 v, \\ v^a &= \mu_1 u, \\ u^c &= \lambda_2 uv, \\ v^c &= \mu_2 v, \end{aligned}$$

for some scalars $\lambda_1$, $\lambda_2$, $\mu_1$ and $\mu_2$.

Let $\delta$ be an element of $\mathbb{F}$ such that

$$\delta^2 = \begin{cases} -2 & \text{if } p^k \equiv 3 \bmod 8, \\ 2 & \text{if } p^k \equiv 7 \bmod 8. \end{cases}$$

Setting $\lambda_1 = \mu_1 = -1$, we find that one solution for $a$ is

$$a := \delta^{-1} \begin{pmatrix} \alpha & \beta + 1 \\ \beta - 1 & -\alpha \end{pmatrix}.$$

Then $a$ has determinant $-1$ or $1$, and its square is $I_2$ or $-I_2$, according as $p^k$ is congruent to 3 or 7 modulo 8, respectively. Setting $\lambda_2 = \mu_2 = -1$, we find that one solution for $c$ is

$$c := \mp\delta^{-1} \begin{pmatrix} -\beta & \alpha + 1 \\ \alpha - 1 & \beta \end{pmatrix},$$

the minus or plus being chosen according as $p^k$ is congruent to 3 or 7 modulo 8, respectively. Then $c$ has determinant $-1$ or 1, and its square is $I_2$ or $-I_2$, according as $p^k$ is congruent to 3 or 7 modulo 8, respectively. Set $b := ac$. Then

$$b = 2^{-1} \begin{pmatrix} \alpha - \beta - 1 & \alpha + \beta - 1 \\ \alpha + \beta + 1 & -\alpha + \beta - 1 \end{pmatrix},$$

and $b$ has determinant 1 and order 3. Furthermore, $b^a = b^2$. We then have the following presentation for $M_3$:

$$\begin{aligned} \{\, a, b, u, v, z \;\mid\; & a^2 = \pm I_2, \\ & b^a = b^2, \quad b^3 = I_2, \\ & u^a = -v, \quad u^b = v, \quad u^2 = -I_2, \\ & v^a = -u, \quad v^b = uv, \quad v^u = -v, \quad v^2 = -I_2, \\ & z^a = z, \quad z^b = z, \quad z^u = z, \quad z^v = z, \quad z^{p^k-1} = I_2 \,\}, \end{aligned}$$

the plus or minus being present in the first relation according as $p^k$ is congruent to 3 or 7 modulo 8, respectively. This is clearly a polycyclic presentation for $M_3$ (after replacing $-I_2$ by $z^{(p^k-1)/2}$). From this presentation we see that

$$\begin{aligned} M_3 &= \langle z \rangle \,\mathsf{Y}\, \langle a, b, u, v \rangle \\ &= \langle z^2 \rangle \times \langle a, b, u, v \rangle \\ &\cong \begin{cases} C_{(p^k-1)/2} \times GL(2,3) & \text{if } p^k \equiv 3 \bmod 8, \\ C_{(p^k-1)/2} \times BO & \text{if } p^k \equiv 7 \bmod 8. \end{cases} \end{aligned}$$

Note that Wilson (1972, Theorem 3.2, p. 36) also observed that $M_3$ splits over its Fitting subgroup when $\mathbb{F}$ has a square root of $-2$ (that is, when $p^k \equiv 3 \bmod 8$).

It is easy to show that $\langle a, b, u, v \rangle$ is the unique minimal supplement to the scalar group, and that

$$\begin{aligned} M_3 \cap SL(2, \mathbb{F}) &= \begin{cases} \langle b, u, v \rangle & \text{if } p^k \equiv 3 \bmod 8, \\ \langle a, b, u, v \rangle & \text{if } p^k \equiv 7 \bmod 8 \end{cases} \\ &\cong \begin{cases} SL(2,3) & \text{if } p^k \equiv 3 \bmod 8, \\ BO & \text{if } p^k \equiv 7 \bmod 8. \end{cases} \end{aligned}$$

Finally, we investigate the action of field automorphisms on $M_3$.

**5.2.1 Theorem.** *Every automorphism of* $\mathbb{F}$*, acting entry-wise on the elements of* $M_3$*, normalises* $M_3$*.*

**Proof.** Let $\theta$ be an automorphism of $\mathbb{F}$. By looking at the entries of the matrices in our generating set for $M_3$, it is clear that the effect of $\theta$ on $M_3$ is determined by $\delta\theta$ (remember that $\alpha$ and $\beta$ belong to the prime subfield of $\mathbb{F}$). Clearly $b$, $u$ and $v$ are fixed by $\theta$ and $a\theta$ is $a$ or $-a$ (and of course $z\theta$ is some power of itself). Therefore $\theta$ normalises $M_3$. ∎

### 5.2.2 A generating set for $M_4$

Recall that $M_4$ is only defined when $p^k \equiv 1 \bmod 4$. We construct a generating set for $M_4$ by the methods described in Section 2.5. Let $z$ be a generator for the scalar group, and define $u$ and $v$ by

$$u := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad v := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then $\{u, v, z\}$ generates the Fitting subgroup of $M_4$. To extend this set to a generating set for $M_4$, we first require a generating set for $Sp(2,2)$. We choose this set to consist of the two elements

$$a\rho := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } b\rho := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

These matrices satisfy the relations

$$(a\rho)^2 = I_2,\ (b\rho)^3 = I_2,\ (b\rho)^{a\rho} = (b\rho)^2.$$

By the theory in Section 2.5, there exist matrices $a$ and $b$ of $GL(2,\mathbb{F})$ satisfying the conditions

$$\begin{aligned} u^a &= \lambda_1 v, \\ v^a &= \mu_1 u, \\ u^b &= \lambda_2 v, \\ v^b &= \mu_2 uv, \end{aligned}$$

for some scalars $\lambda_1$, $\lambda_2$, $\mu_1$ and $\mu_2$.

Let $\omega$ be a primitive 4-th root of unity in $\mathbb{F}$, and let $\delta$ be an element of $\mathbb{F}$ such that

$$\delta^2 := \begin{cases} -2 & \text{if } p^k \equiv 1 \bmod 8, \\ -2\omega & \text{if } p^k \equiv 5 \bmod 8. \end{cases}$$

Setting $\lambda_1 = \mu_1 = -1$, we find that one solution for $a$ is

$$a := \delta^{-1} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}.$$

If $p^k \equiv 1 \bmod 8$, then $a$ has determinant 1 and its square is $-I_2$. If $p^k \equiv 5 \bmod 8$, then $a$ has determinant $-\omega$ and its square is $\omega I_2$. Setting $\lambda_2 = 1$ and $\mu_2 = \omega$, we find that one solution for $b$ is

$$b := 2^{-1} \begin{pmatrix} \omega - 1 & \omega + 1 \\ \omega - 1 & -\omega - 1 \end{pmatrix}.$$

Then $b$ has determinant 1 and order 3, and $b^a = b^2$.

We then have the following presentation for $M_4$:

$$\begin{aligned} \{\, a, b, u, v, z \;\mid\; & a^2 = \sigma I_2, \\ & b^a = b^2, \quad b^3 = I_2, \\ & u^a = -v, \quad u^b = v, \quad u^2 = I_2, \\ & v^a = -u, \quad v^b = \omega uv, \quad v^u = -v, \quad v^2 = I_2 \\ & z^a = z, \quad z^b = z, \quad z^u = z, \quad z^v = z, \quad z^{p^k-1} = I_2 \,\}, \end{aligned}$$

where $\sigma$ is $-1$ or $\omega$, according as $p^k$ is congruent to 1 or 5 modulo 8, respectively. Since $b$ does not normalise $\langle u, v \rangle$, it is more convenient to work with $\langle \omega u, \omega v \rangle$. Setting $x := \omega u$ and $y := \omega v$, we then have

$$\begin{aligned} \{\, a, b, x, y, z \;\mid\; & a^2 = \sigma I_2, \\ & b^a = b^2, \quad b^3 = I_2, \\ & x^a = -y, \quad x^b = y, \quad x^2 = -I_2, \\ & y^a = -x, \quad y^b = xy, \quad y^x = -y, \quad y^2 = -I_2, \\ & z^a = z, \quad z^b = z, \quad z^x = z, \quad z^y = z, \quad z^{p^k-1} = I_2 \,\}, \end{aligned}$$

which is clearly a polycyclic presentation for $M_4$ (after replacing $-I_2$ by $z^{(p^k-1)/2}$ and, if necessary, $\omega I_2$ by $z^{(p^k-1)/4}$). From this presentation we see that

$$\begin{aligned} M_4 &= \langle z \rangle \,\Upsilon\, \langle a, b, x, y \rangle \\ &= \begin{cases} \langle z \rangle \,\Upsilon\, \langle a, b, x, y \rangle & \text{if } p^k \equiv 1 \bmod 8, \\ \langle z^4 \rangle \times \langle a, b, x, y \rangle & \text{if } p^k \equiv 5 \bmod 8 \end{cases} \\ &\cong \begin{cases} C_{p^k-1} \,\Upsilon\, BO & \text{if } p^k \equiv 1 \bmod 8, \\ C_{(p^k-1)/4} \times NS & \text{if } p^k \equiv 5 \bmod 8. \end{cases} \end{aligned}$$

It is easy to show that $\langle a, b, x, y\rangle$ is a minimal supplement to the scalar group. If $p^k \equiv 5 \bmod 8$, then it is the unique such supplement. If $p^k \equiv 1 \bmod 8$, then there is just one other minimal supplement to the scalar group; it is $\langle \omega a, b, x, y\rangle$, which is isomorphic to $GL(2,3)$. Note that Wilson (1972, Theorem 3.2, p. 36) also observed that $M_4$ splits over its Fitting subgroup when $\mathbb{F}$ has a square root of $-2$ (that is, when $p^k \equiv 1 \bmod 8$).

Also, we have that

$$M_4 \cap SL(2,\mathbb{F}) = \begin{cases} \langle a, b, x, y\rangle & \text{if } p^k \equiv 1 \bmod 8, \\ \langle b, x, y\rangle & \text{if } p^k \equiv 5 \bmod 8 \end{cases}$$
$$\cong \begin{cases} BO & \text{if } p^k \equiv 1 \bmod 8, \\ SL(2,3) & \text{if } p^k \equiv 5 \bmod 8. \end{cases}$$

Finally, we investigate the action of field automorphisms on $M_4$.

**5.2.2 Theorem.** *Every automorphism of $\mathbb{F}$, acting entry-wise on the elements of $M_4$, normalises $M_4$.*

**Proof.** Let $\theta$ be an automorphism of $\mathbb{F}$. By looking at the entries of the matrices in our generating set for $M_4$, it is clear that the effect of $\theta$ on $M_4$ is determined by $\omega\theta$ and $\delta\theta$. It is not difficult to check that, in any case, $x\theta$ is $\pm x$, $y\theta$ is $\pm y$, $a\theta$ is $\pm\omega a$, and $b\theta$ is $b$ or $by$ (and of course $z\theta$ is some power of itself). Therefore $\theta$ normalises $M_4$. ■

## 5.3 The primitive subgroups of $M_3$ and $M_4$

**5.3.1 Theorem.** (L. G. Kovács) *If $G$ is an abelian-by-nilpotent primitive subgroup of $GL(n,\mathbb{F})$, then $G$ normalises a Singer cycle.*

**Proof.** If $G$ is abelian, then it is cyclic, and the result follows from Theorem 2.3.3. Now assume that $G$ is not abelian. Let $A$ be maximal among the abelian normal subgroups of $G$ whose quotient is nilpotent. Set $C := \mathbf{C}_{GL(n,\mathbb{F})}(G)$. Since $G$ is irreducible, we have that $C$ is the multiplicative group of a field, say $\mathbb{K} = GF(p^{km})$, where $m \mid n$. Then $\mathbf{C}_{GL(n,\mathbb{F})}(C) = GL(n/m, \mathbb{K})$, and $G$ is primitive and absolutely irreducible as subgroup of $GL(n/m, \mathbb{K})$.

Under a suitable extension $\mathbb{L}$ of $\mathbb{K}$, $A$ becomes diagonalisable and so normalises each member of a certain set of $n/m$ 1-dimensional $\mathbb{L}$-spaces which generate the vector space $V(n/m, \mathbb{L})$. Since $G$ is absolutely irreducible as subgroup of $GL(n/m, \mathbb{K})$, it follows that $G$ permutes these spaces transitively. Therefore, by the Orbit-Stabiliser Theorem, $|G\colon A| \geq n/m$.

Since $G$ is primitive as subgroup of $GL(n/m, \mathbb{K})$, it follows that the $\mathbb{K}$-linear span of $A$ is a field, say $\mathbb{E} = GF(p^{klm})$, where $l \mid \frac{n}{m}$. There is a homomorphism from $G$ to the Galois group of $\mathbb{E}$ over $\mathbb{K}$ whose kernel is $\mathbf{C}_G(A)$. In particular, $G/\mathbf{C}_G(A)$ is cyclic of order dividing $l$. From Theorem 3.2.5, and from the maximality of $A$, we deduce that $\mathbf{C}_G(A) = A$. Therefore $|G\colon A| \leq l$. This shows that $n/m = |G\colon A| = l$. In particular, $\mathbb{E} = GF(p^{kn})$, and so the multiplicative group of $\mathbb{E}$ is a Singer cycle of $GL(n, \mathbb{F})$. Since $G$ normalises $A$, it also normalises $\mathbb{E}$. This completes the proof. ■

**5.3.2 Corollary.** *A primitive subgroup of $GL(2, \mathbb{F})$ is conjugate to a subgroup of the normaliser of a Singer cycle if and only if it is cyclic or has a cyclic subgroup of index 2.* ■

### 5.3.1 The case $p^k \equiv 3 \bmod 8$

Recall that $M_3 \cong C_{(p^k-1)/2} \times GL(2,3)$.

**5.3.3 Theorem.** *The following is a complete and irredundant list of $GL(2, \mathbb{F})$-conjugacy class representatives of the primitive soluble subgroups of $GL(2, \mathbb{F})$ whose guardian is $M_3$:*

$$\begin{aligned} &\langle a, b, u, v, z^{2i} \rangle, && i \mid (p^k - 1)/2; \\ &\langle b, u, v, z^{2j} \rangle, && j \mid (p^k - 1)/2; \\ &\langle bz^{2l}, u, v \rangle, && l \mid (p^k - 1)/6, \end{aligned}$$

*where the last row of groups exists if and only if $3 \mid (p^k - 1)$.*

**Proof.** Let $G$ be a primitive subgroup of $M_3$ which is not conjugate to a subgroup of the normaliser of a Singer cycle. Let $A$ be the scalar group, set $B := O_{2'}(A) = \langle z^2 \rangle$, and set $N := \langle a, b, u, v \rangle$. Then $N \cong GL(2,3)$ and $M_3 = N \times B$. By Theorem 3.2.2,

we can parametrise $G$ by the triple $(N_1/N_0, B_1/B_0, \theta)$, where $N_1 = N \cap GB$, $N_0 = N \cap G$, $B_1 = NG \cap B$, $B_0 = G \cap B$, and $\theta$ is an isomorphism from $N_1/N_0$ to $B_1/B_0$. From Proposition 5.1.1, $N_1$ is primitive. Refer to Figure 5.1 for the Burnside lattice of $N$. If $N_1$ were abelian, then $G$ would be abelian and so conjugate to a subgroup of a Singer cycle, a contradiction. So $N_1$ is not abelian. Suppose $N_1$ is $D_{12}$. Then $D_{12}$ is primitive, and so its subgroup isomorphic to $C_6$ is irreducible, by Clifford's Theorem. In particular, $3 \nmid (p^k - 1)$. This implies that $D_{12} \times B$ has a cyclic subgroup of index 2. But then $G$ is conjugate to a subgroup of the normaliser of a Singer cycle, a contradiction. Therefore $N_1$ is not $D_{12}$. The same argument prevents $N_1$ from being $S_3$, $SD_{16}$, $D_8$ or $Q_8$. So $N_1$ may be either $GL(2,3)$ or $SL(2,3)$. Each of these groups is irreducible and does not have an abelian subgroup of index 2, and consequently is primitive and not conjugate to a subgroup of the normaliser of a Singer cycle.

Suppose that $N_1$ is $GL(2,3)$. Then $N_0$ is $GL(2,3)$, as this is the only normal subgroup of $GL(2,3)$ whose quotient is cyclic of odd order. Then $B_0 = B_1$, and $G = GL(2,3) \times B_1$. Thus $G$ belongs to the first row of groups in the statement of the theorem.

Suppose that $N_1$ is $SL(2,3)$. Then $N_0$ is either $SL(2,3)$ or $Q_8$, as these are the only normal subgroups of $SL(2,3)$ whose quotients are cyclic of odd order. If $N_0$ is $SL(2,3)$, then $B_0 = B_1$, and $G = SL(2,3) \times B_1$. Thus $G$ belongs to the second row of groups in the theorem. If $N_0$ is $Q_8$, then $3 | (p^k - 1)$, and $G$ is one of the two diagonals between $Q_8 \times B_0$ and $SL(2,3) \times B_1$, where $|B_1/B_0| = 3$. However, these two diagonals are conjugate in $M_3$, because the elements of order 3 in $GL(2,3)$ lie in a single conjugacy class. Thus, without loss of generality, $G$ belongs to the third row of groups.

We have proved that the above list is complete. The information in Table 5.1 shows that no two groups on it are conjugate in $GL(2,\mathbb{F})$. In this table we use the notation $G_{ij}$ to mean the group from row $i$ with parameter $j$. ■

### 5.3.2 The case $p^k \equiv 7 \bmod 8$

Recall that $M_3 \cong C_{(p^k-1)/2} \times BO$.

| $G$ | $\lvert G\rvert$ | $G \cap SL(2,\mathbb{F})$ | $\lvert G \cap A\rvert$ |
|---|---|---|---|
| $G_{1i}$ | $24(p^k-1)/i$ | $SL(2,3)$ | $(p^k-1)/i$ |
| $G_{2j}$ | $12(p^k-1)/j$ | $SL(2,3)$ | $(p^k-1)/j$ |
| $G_{3l}$ | $4(p^k-1)/l$ | $Q_8$ | $(p^k-1)/3l$ |

Table 5.1: Information on some primitive subgroups of $M_3$, $p^k \equiv 3 \bmod 8$

**5.3.4 Theorem.** *The following is a complete and irredundant list of $GL(2,\mathbb{F})$-conjugacy class representatives of the primitive soluble subgroups of $GL(2,\mathbb{F})$ whose guardian is $M_3$:*

$$\begin{aligned} &\langle a, b, u, v, z^{2i}\rangle, && i \,|\, (p^k-1)/2\,; \\ &\langle b, u, v, z^{2j}\rangle, && j \,|\, (p^k-1)/2\,; \\ &\langle bz^{2l}, u, v\rangle, && l \,|\, (p^k-1)/6, \end{aligned}$$

*where the last row of groups exists if and only if $3 \,|\, (p^k-1)$.*

**Proof.** This proof is entirely similar to that of Theorem 5.3.3. Note that the elements of $BO$ of order 3 lie in a single conjugacy class. The relevant table is Table 5.2. ■

| $G$ | $\lvert G\rvert$ | $G \cap SL(2,\mathbb{F})$ | $\lvert G \cap A\rvert$ |
|---|---|---|---|
| $G_{1i}$ | $24(p^k-1)/i$ | $BO$ | $(p^k-1)/i$ |
| $G_{2j}$ | $12(p^k-1)/j$ | $SL(2,3)$ | $(p^k-1)/j$ |
| $G_{3l}$ | $4(p^k-1)/l$ | $Q_8$ | $(p^k-1)/3l$ |

Table 5.2: Information on some primitive subgroups of $M_3$, $p^k \equiv 7 \bmod 8$

### 5.3.3 The case $p^k \equiv 1 \bmod 8$

Recall that $M_4 \cong C_{p^k-1} \curlyvee BO$.

**5.3.5 Theorem.** *If $G$ is a primitive subgroup of $M_4$ which does not contain the scalar matrix $-I_2$, then $G$ is conjugate to a subgroup of the normaliser of a Singer cycle.*

**Proof.** Let $G$ be a primitive subgroup of $M_4$ which does not contain the scalar matrix $-I_2$. From the Burnside lattice of $BO$ (see Figure 5.2) we see that there are only two classes of subgroups of $BO$ that do not contain the centre; they are the trivial group and the cyclic groups of order 3. Hence $G \cap BO$ is trivial or a $C_3$. If $G \cap BO = 1$, then $G$ is cyclic and therefore conjugate to a subgroup of a Singer cycle. Suppose that $G \cap BO = H$, where $|H| = 3$. Then $H \trianglelefteq G$, and so by Clifford's Theorem, $H$ is irreducible or scalar. But of course it is not scalar, and so $H$ is irreducible. Then $\mathbf{C}_G(H)$ is cyclic, and has index 1 or 2 in $G$ because $\mathrm{Aut}(H) = 2$. The result now follows from Corollary 5.3.2. ∎

**5.3.6 Theorem.** *The following is a complete and irredundant list of $GL(2,\mathbb{F})$-conjugacy class representatives of the primitive soluble subgroups of $GL(2,\mathbb{F})$ whose guardian is $M_4$:*

$$\begin{aligned}
&\langle a, b, x, y, z^i \rangle, && i \,|\, (p^k - 1)/2\,; \\
&\langle az^j, b, x, y \rangle, && j \,|\, (p^k - 1)/4\,; \\
&\langle b, x, y, z^l \rangle, && l \,|\, (p^k - 1)/2\,; \\
&\langle bz^m, x, y \rangle, && m \,|\, (p^k - 1)/6,
\end{aligned}$$

*where the last row of groups exists if and only if $3 \,|\, (p^k - 1)$.*

**Proof.** This proof is entirely similar to that of Theorem 5.3.3. Note that since $p^k \equiv 1 \bmod 4$, it follows that the JS-imprimitive discussed in Chapter 3 is a Sylow 2-subgroup of $GL(2,\mathbb{F})$, and so the 2-subgroups of $BO$ are imprimitive. Note also that the elements of $BO$ of order 3 lie in a single conjugacy class. The relevant table is Table 5.3. ∎

| $G$ | $\lvert G\rvert$ | $G \cap SL(2,\mathbb{F})$ | $\lvert G \cap A\rvert$ |
|---|---|---|---|
| $G_{1i}$ | $24(p^k-1)/i$ | $BO$ | $(p^k-1)/i$ |
| $G_{2j}$ | $12(p^k-1)/j$ | $SL(2,3)$ | $(p^k-1)/2j$ |
| $G_{3l}$ | $12(p^k-1)/l$ | $SL(2,3)$ | $(p^k-1)/l$ |
| $G_{4m}$ | $4(p^k-1)/m$ | $Q_8$ | $(p^k-1)/3m$ |

Table 5.3: Information on some primitive subgroups of $M_4$, $p^k \equiv 1 \bmod 8$

### 5.3.4 The case $p^k \equiv 5 \bmod 8$

Recall that $M_4 \cong C_{(p^k-1)/4} \times NS$.

**5.3.7 Theorem.** *The following is a complete and irredundant list of $GL(2,\mathbb{F})$-conjugacy class representatives of the primitive soluble subgroups of $GL(2,\mathbb{F})$ whose guardian is $M_4$:*

$$\begin{aligned}
&\langle a, b, x, y, z^{4i}\rangle, && i \,|\, (p^k-1)/4\,;\\
&\langle a^2, b, x, y, z^{4j}\rangle, && j \,|\, (p^k-1)/4\,;\\
&\langle a^2, bz^{4l}, x, y\rangle, && l \,|\, (p^k-1)/12\,;\\
&\langle b, x, y, z^{4m}\rangle, && m \,|\, (p^k-1)/4\,;\\
&\langle bz^{4n}, x, y\rangle, && n \,|\, (p^k-1)/12,
\end{aligned}$$

*where the groups in the third and fifth rows exist if and only if $3 \,|\, (p^k-1)$.*

**Proof.** This proof is entirely similar to that of Theorem 5.3.3. Note that since $p^k \equiv 1 \bmod 4$, it follows that the JS-imprimitive discussed in Chapter 3 is a Sylow 2-subgroup of $GL(2,\mathbb{F})$, and so the 2-subgroups of $NS$ are imprimitive. Note also that the elements of $NS$ of order 3 lie in a single conjugacy class. The relevant table is Table 5.4. ∎

| $G$ | $\lvert G\rvert$ | $G \cap SL(2,\mathbb{F})$ | $\lvert G \cap A\rvert$ |
|---|---|---|---|
| $G_{1i}$ | $24(p^k-1)/i$ | $SL(2,3)$ | $(p^k-1)/i$ |
| $G_{2j}$ | $12(p^k-1)/j$ | $SL(2,3)$ | $(p^k-1)/j$ |
| $G_{3l}$ | $4(p^k-1)/l$ | $Q_8$ | $(p^k-1)/3l$ |
| $G_{4m}$ | $6(p^k-1)/m$ | $SL(2,3)$ | $(p^k-1)/2m$ |
| $G_{5n}$ | $2(p^k-1)/n$ | $Q_8$ | $(p^k-1)/6n$ |

Table 5.4: Information on some primitive subgroups of $M_4$, $p^k \equiv 5 \bmod 8$

# Chapter 6

# Some irreducible soluble subgroups of $GL(q, p^k)$, $q > 2$

If $q$ is an odd prime, then the only numbers of the form $p^q$ that are less than 256 are $2^3$, $3^3$, $5^3$, $2^5$, $3^5$ and $2^7$. By Remark 2.5.5, there are no imprimitive subgroups of $GL(q, 2)$, and by Remark 2.5.18, the only JS-primitive of $GL(q, p)$ for the above values of $p$ and $q$ is the normaliser of a Singer cycle. In Chapter 4 we gave a list of all the primitive subgroups and irreducible cyclic subgroups of that JS-primitive. Therefore, it remains only to determine the imprimitive soluble subgroups of $GL(3, 3)$, $GL(3, 5)$ and $GL(5, 3)$. We carry out those determinations later in this chapter, after discussing some general aspects of the JS-maximals of $GL(q, p^k)$. Also in this chapter we obtain a generating set for one of the JS-primitives of $GL(3, p^k)$. This set is used in Chapter 9 to obtain a generating set for one of the JS-primitives of $GL(6, 2)$.

## 6.1 The JS-maximals of $GL(q, p^k)$

In Chapters 3, 4 and 5 we gave theorems which provide a complete and irredundant list of conjugacy class representatives of the irreducible soluble subgroups of $GL(2, p^k)$. In this section we discuss how far we can extend those methods to cover the irreducible soluble subgroups of other prime degrees.

Let $q$ be an odd prime. By Remark 2.1.7, there is a unique conjugacy class

of transitive maximal soluble subgroups of $S_q$, namely $\mathrm{Hol}(C_q)$. Therefore there is just one JS-imprimitive of $GL(q,p^k)$, namely,

$$M_1(q,p^k) := GL(1,p^k) \operatorname{wr} \mathrm{Hol}(C_q)\,, \quad p^k \neq 2\,.$$

If $G$ is an irreducible subgroup of $M_1$, then the projection of $G$ into the top group contains $C_q$. Consequently, $G$ contains a normal subgroup $H$ that is conjugate to a subgroup of $GL(1,p^k) \operatorname{wr} C_q$. Since the degree is prime, it follows from Clifford's Theorem that $H$ is irreducible. So the analysis of the irreducible subgroups of $M_1$ should begin with the analysis of the irreducible subgroups of $GL(1,p^k) \operatorname{wr} C_q$. The methods of Chapter 3 should extend to this group without too much trouble. The difficulty of finding the irreducible subgroups of $M_1$ that are not contained in $GL(1,p^k) \operatorname{wr} C_q$ clearly depends on the prime factorisation of $q-1$. For the first few primes, one should be able to obtain the desired list, and by so doing one may find a method of providing a list for all $q$. Note that Conlon (1977) has determined the non-abelian $q$-subgroups of the general linear group of degree $q$ over an arbitrary field.

There is one JS-primitive of $GL(q,p^k)$ whose unique maximal abelian normal subgroup has order $p^{kq}-1$, namely,

$$M_2(q,p^k) := C_{p^{kq}-1} \rtimes C_q\,,$$

the normaliser of a Singer cycle. From Chapter 4, we have a complete and irredundant list of $GL(q,p^k)$-conjugacy class representatives of the primitive subgroups and imprimitive cyclic subgroups of this group.

The remaining JS-primitives of $GL(q,p^k)$ have the scalar group $A$ as their unique maximal abelian normal subgroup, and are written as

$$(A \curlyvee E) \lrcorner D\,, \quad q \mid (p^k-1)\,,$$

where $E$ is extraspecial of order $q^3$ and exponent $q$, and $D$ is a maximal irreducible soluble subgroup of $Sp(2,q)$. As pointed out by Suprunenko (1976, p. 165), the maximal irreducible soluble subgroups of $Sp(2,q)$ are found by intersecting $Sp(2,q)$ with the maximal irreducible soluble subgroups of $GL(2,q)$. Suprunenko (1976, pp. 165-167) calculates the orders of these intersections, and finds that the only primes they involve are divisors of $q-1$ or $q+1$.

6.1.1 Theorem. *Let $q$ be an odd prime dividing $p^k - 1$, and let $M$ be one of the JS-primitives of $GL(q, p^k)$ that we describe as*

$$(A \Upsilon E) \downharpoonright D,$$

*where $A$ is the scalar group, $E$ is extraspecial of order $q^3$ and exponent $q$, and $D$ is a maximal irreducible soluble subgroup of $Sp(2, q)$. Then $M$ can also be written as*

$$A \Upsilon (E \rtimes D).$$

**Proof.** Refer to Figure 6.1. In Section 6.5 this theorem is proved by construction for $q = 3$, so let us assume that $q > 3$. Let $n$ be the order of $D$, so that the order of $M$ is $nq^2(p^k - 1)$. As mentioned above, Suprunenko shows that the only primes involved in $n$ are divisors of $q - 1$ or $q + 1$. Set $N := M \cap SL(q, p^k)$; note that $N \geq E$ (by inspection of the matrices used to generate $E$). It is clear that $|M : N|$ is $p^k - 1$ or $(p^k - 1)/q$. If the former were true, then $AN$ would be a subgroup of $M$ of index $q$ that contains $AE$; this contradicts the fact that $n$ and $q$ are coprime. Therefore $|M : N| = (p^k - 1)/q$, and $M = A \Upsilon N$. It then follows from the Schur-Zassenhaus Theorem that $N = E \rtimes D$. ∎

Note that the order of $E \rtimes D$ is independent of $p^k$. Therefore we can use the methods of Chapter 5 to find the primitive subgroups of $M$ in the above theorem: if we know the primitive subgroups of $E \rtimes D$ and some structural information, such as their normal subgroups with cyclic quotients, and the number of conjugacy classes of elements of certain orders, then we know all the primitive subgroups of $M$. Hence we essentially have (modulo investigation of the groups $E \rtimes D$, and finding generating sets for them) a list of the primitive soluble subgroups of $GL(q, p^k)$. Of course, this list depends on the structures of the groups $E \rtimes D$ and so we need a different list for each $q$.

## 6.2 The imprimitive soluble subgroups of $GL(3, 3)$

Let $M$ be the JS-imprimitive of $GL(3, 3)$, that is,

$$M := GL(1, 3) \operatorname{wr} S_3.$$

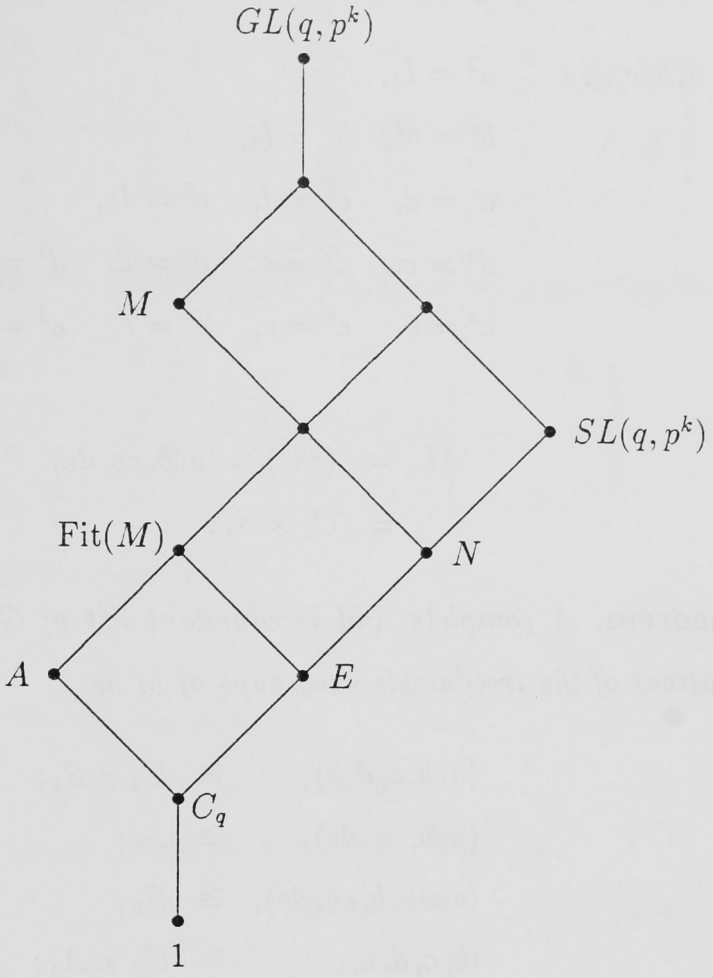



Figure 6.1: Part of the lattice of $M$

This group has order 48, and is generated by the matrices

$$a := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; b := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } \; c := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In order to obtain a polycyclic presentation for $M$ we introduce the elements

$$d := c^b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \; e := d^b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then a polycyclic presentation for $M$ is

$$\begin{aligned}\{\, a,b,c,d,e \;\mid\; & a^2 = I_3, \\ & b^a = b^2,\quad b^3 = I_3, \\ & c^a = d,\quad c^b = d,\quad c^2 = I_3, \\ & d^a = c,\quad d^b = e,\quad d^c = d,\quad d^2 = I_3, \\ & e^a = e,\quad e^b = c,\quad e^c = e,\quad e^d = e,\quad e^2 = I_3 \,\}\,.\end{aligned}$$

Note that

$$\begin{aligned} M &= \langle cde \rangle \times \langle a, b, ce, de \rangle \\ &\cong C_2 \times S_4\,. \end{aligned}$$

**6.2.1 Theorem.** *A complete and irredundant list of $GL(3,3)$-conjugacy class representatives of the irreducible subgroups of $M$ is:*

$$\begin{aligned} \langle a,b,c,d,e \rangle, &\quad \cong C_2 \times S_4\,; \\ \langle a,b,ce,de \rangle, &\quad \cong S_4\,; \\ \langle acde,b,ce,de \rangle, &\quad \cong S_4\,; \\ \langle b,c,d,e \rangle, &\quad \cong C_2 \times A_4\,; \\ \langle b,ce,de \rangle, &\quad \cong A_4\,. \end{aligned}$$

**Proof.** It is not difficult to show that the irreducible subgroups of $\langle a,b,ce,de \rangle$ are $S_4$ and $A_4$. The proof now proceeds in the same way as that of Theorem 5.3.3. It is easy to verify the claims about the isomorphism types of the groups listed. Therefore, to show that the list is irredundant, we only need to establish that the second and third groups are not conjugate in $GL(3,3)$. This can be seen by looking at the determinants of the matrices in their respective generating sets: the third group in the theorem is clearly a subgroup of $SL(3,3)$, whereas the second group is not. ■

## 6.3 The imprimitive soluble subgroups of $GL(3,5)$

Let $M$ be the JS-imprimitive of $GL(3,5)$, that is,

$$M := GL(1,5) \operatorname{wr} S_3\,.$$

This group has order 384, and is generated by the matrices

$$a := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; b := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } \; c := \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In order to obtain a polycyclic presentation for $M$ we introduce the elements

$$d := c^b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \; e := d^b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then a polycyclic presentation for $M$ is

$$\begin{aligned} \{ a, b, c, d, e \;\; | \;\; & a^2 = I_3, \\ & b^a = b^2, \quad b^3 = I_3, \\ & c^a = d, \quad c^b = d, \quad c^4 = I_3, \\ & d^a = c, \quad d^b = e, \quad d^c = d, \quad d^4 = I_3, \\ & e^a = e, \quad e^b = c, \quad e^c = e, \quad e^d = e, \quad e^4 = I_3 \}. \end{aligned}$$

Note that

$$\begin{aligned} M &= \langle cde \rangle \times \langle a(cde)^2, b, ce^{-1}, de^{-1} \rangle \\ &= \langle cde \rangle \times (M \cap SL(3,5)). \end{aligned}$$

**6.3.1 Theorem.** *A complete and irredundant list of $GL(3,5)$-conjugacy class representatives of the irreducible subgroups of $M$ is:*

$$\begin{aligned} &\langle a(cde)^2, b, ce^{-1}, de^{-1}, (cde)^i \rangle, && i = 1, 2, 4; \\ &\langle a(cde)^{2+j}, b, ce^{-1}, de^{-1} \rangle, && j = 1, 2; \\ &\langle b, ce^{-1}, de^{-1}, (cde)^k \rangle, && k = 1, 2, 4; \\ &\langle a(cde)^2, b, (ce^{-1})^2, (de^{-1})^2, (cde)^l \rangle, && l = 1, 2, 4; \\ &\langle a(cde)^{2+m}, b, (ce^{-1})^2, (de^{-1})^2 \rangle, && m = 1, 2; \\ &\langle b, (ce^{-1})^2, (de^{-1})^2, (cde)^n \rangle, && n = 1, 2, 4. \end{aligned}$$

**Proof.** Set $B := \langle cde \rangle$ and $N := M \cap SL(3,5)$. We use the CAYLEY function lattice to obtain the subgroup lattice of $N$. If a subgroup of $N$ is irreducible, then its projection into the top group must be transitive. Therefore the 2-subgroups of $N$ are reducible. This leaves just six conjugacy classes of subgroups to consider,

the groups in those classes being isomorphic to one of $N$, 48.52 (this is the number of that group in the tables of Neubüser (1967)), $S_4$, $A_4$, $S_3$ or $C_3$. It is not difficult to show, then, that the only irreducible subgroups of $N$ are $N$, 48.52, $S_4$ and $A_4$. The proof now proceeds in the same way as that of Theorem 5.3.3. Note that none of these groups has a normal subgroup of index 4, and that 48.52 has no subgroup of index 2. The relevant table is Table 6.1. ■

| $G$ | $\lvert G\rvert$ | $G \cap SL(3,5)$ | $\lvert G \cap B\rvert$ |
|---|---|---|---|
| $G_{1i}$ | $384/i$ | $N$ | $4/i$ |
| $G_{2j}$ | $192/j$ | 48.52 | $2/j$ |
| $G_{3k}$ | $192/k$ | 48.52 | $4/k$ |
| $G_{4l}$ | $96/l$ | $S_4$ | $4/l$ |
| $G_{5m}$ | $48/m$ | $A_4$ | $2/m$ |
| $G_{6n}$ | $48/n$ | $A_4$ | $4/n$ |

Table 6.1: Information on the imprimitive soluble subgroups of $GL(3,5)$

## 6.4 The imprimitive soluble subgroups of $GL(5,3)$

Let $M$ be the JS-imprimitive of $GL(5,3)$, that is,

$$M := GL(1,3) \operatorname{wr} \mathrm{Hol}(C_5)\,.$$

By the same methods as in the previous two sections we can write down a polycyclic presentation for $M$, namely $M = \langle a,b,c,d,e,f,g\rangle$, where

$$\begin{aligned}
&a^4 = I_5,\\
&b^a = b^2,\quad b^5 = I_5,\\
&c^a = d,\quad c^b = d,\quad c^2 = I_5,\\
&d^a = f,\quad d^b = e,\quad d^c = d,\quad d^2 = I_5,\\
&e^a = c,\quad e^b = f,\quad e^c = e,\quad e^d = e,\quad e^2 = I_5,\\
&f^a = e,\quad f^b = g,\quad f^c = f,\quad f^d = f,\quad f^e = f,\quad f^2 = I_5,\\
&g^a = g,\quad g^b = c,\quad g^c = g,\quad g^d = g,\quad g^e = g,\quad g^f = g,\quad g^2 = I_5\,.
\end{aligned}$$

We do not write down the matrices referred to in this presentation, as it is obvious what they are. We mention, however, that $b$ has determinant 1 and that the other members of the generating set have determinant 2. Note that

$$\begin{aligned} M &= \langle cdefg \rangle \times \langle acdefg, b, cd, de, ef, fg \rangle \\ &= \langle cdefg \rangle \times (M \cap SL(5,3)) . \end{aligned}$$

**6.4.1 Theorem.** *A complete and irredundant list of $GL(5,3)$-conjugacy class representatives of the irreducible subgroups of $M$ is:*

$$\begin{aligned} &\langle acdefg, b, cd, de, ef, fg, (cdefg)^i \rangle, && i = 1, 2; \\ &\langle a, b, cd, de, ef, fg \rangle; \\ &\langle a^2, b, cd, de, ef, fg, (cdefg)^j \rangle, && j = 1, 2; \\ &\langle a^2 cdefg, b, cd, de, ef, fg \rangle; \\ &\langle b, cd, de, ef, fg, (cdefg)^k \rangle, && k = 1, 2. \end{aligned}$$

**Proof.** Set $B := \langle cdefg \rangle$ and $N := \langle a, b, cd, de, ef, fg \rangle$. We use the CAYLEY function lattice to obtain the subgroup lattice of $N$. If a subgroup of $N$ is irreducible, then its projection into the top group must be transitive. Therefore the 2-subgroups of $N$ are reducible. This leaves just six conjugacy classes of subgroups to consider, the groups in those classes being isomorphic to one of $N$, $\frac{1}{2}N$ (meaning the unique subgroup of $N$ of index 2), $\frac{1}{4}N$ (meaning the unique subgroup of $N$ of index 4), $\mathrm{Hol}(C_5)$, $D_{10}$ or $C_5$. It is not difficult to show, then, that the only irreducible subgroups of $N$ are $N$, $\frac{1}{2}N$ and $\frac{1}{4}N$. The proof now proceeds in the same way as that of Theorem 5.3.3. The relevant table is Table 6.2. ∎

| $G$ | $\lvert G \rvert$ | $G \cap SL(5,3)$ | $\lvert G \cap B \rvert$ |
|---|---|---|---|
| $G_{1i}$ | $640/i$ | $N$ | $2/i$ |
| $G_2$ | 320 | $\frac{1}{2}N$ | 1 |
| $G_{3j}$ | $320/j$ | $\frac{1}{2}N$ | $2/j$ |
| $G_4$ | 160 | $\frac{1}{4}N$ | 1 |
| $G_{5k}$ | $160/k$ | $\frac{1}{4}N$ | $2/k$ |

Table 6.2: Information on the imprimitive soluble subgroups of $GL(5,3)$

## 6.5 A generating set for a JS-primitive of $GL(3, p^k)$

Let $\mathbb{F}$ be the field of $p^k$ elements, where $p^k \equiv 1 \bmod 3$. Since $Sp(2,3)$ is soluble, it follows that there is at just one JS-primitive of $GL(3,\mathbb{F})$ whose unique maximal abelian normal subgroup has order $p^k - 1$, namely

$$M := (C_{p^k-1} \curlyvee E) \lhd Sp(2,3)\,,$$

where $E$ is extraspecial of order 27 and exponent 3. In this section we derive a polycyclic presentation for $M$, from which we see that $M = C_{p^k-1} \curlyvee (E \rtimes Sp(2,3))$. This provides a constructive proof of Theorem 6.1.1 in the case $q = 3$. We also need this presentation in Chapter 9 when we derive a presentation for one of the JS-primitives of $GL(6,2)$.

We construct a generating set for $M$ by the methods described in Section 2.5. Let $z$ be a generator for the scalar group, and define $u$ and $v$ by

$$u := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad v := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^2 \end{pmatrix},$$

where $\varepsilon$ is a primitive cube root of unity in $\mathbb{F}$. Then $\{u, v, z\}$ generates $\mathrm{Fit}(M)$. To extend this set to a generating set for $M$, we first require a generating set for $Sp(2,3)$. The set we use consists of the three matrices

$$a\rho := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; b\rho := \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad c\rho := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

These matrices satisfy the following relations:

$$\begin{aligned} &(a\rho)^3 = 1, \\ &(b\rho)^{a\rho} = c\rho, \quad (b\rho)^2 = (c\rho)^2, \\ &(c\rho)^{a\rho} = b\rho c\rho, \quad (c\rho)^{b\rho} = (c\rho)^3, \quad (c\rho)^4 = 1\,. \end{aligned}$$

By the theory in Section 2.5, there exist matrices $a$, $b$ and $c$ of $GL(3,\mathbb{F})$ such that

$$\begin{aligned} u^a &= \lambda_1 uv^2, \quad & u^b &= \lambda_2 uv, \quad & u^c &= \lambda_3 u^2 v, \\ v^a &= \mu_1 v, \quad & v^b &= \mu_2 uv^2, \quad & v^c &= \mu_3 uv, \end{aligned}$$

where the $\lambda_i$ and $\mu_j$ are scalars. Setting $\lambda_3 = \mu_3 = \varepsilon^2$ we find that one solution for $c$ is

$$c := (1-\varepsilon)^{-1} \begin{pmatrix} 1 & \varepsilon & \varepsilon \\ \varepsilon & 1 & \varepsilon \\ 1 & 1 & \varepsilon^2 \end{pmatrix}.$$

Then $c$ has determinant 1 and order 4. Setting $\lambda_2 = 1$ and $\mu_2 = \varepsilon^2$ we find that one solution for $b$ is

$$b := (1-\varepsilon)^{-1} \begin{pmatrix} 1 & \varepsilon & 1 \\ \varepsilon & 1 & 1 \\ \varepsilon & \varepsilon & \varepsilon^2 \end{pmatrix}.$$

Then $b$ has determinant 1, $b^2 = c^2$ and $c^b = c^3$. Setting $\lambda_1 = \mu_1 = 1$ we find that one solution for $a$ is

$$a := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}.$$

Then $a$ has determinant $\varepsilon$ and order 3, and $b^a = c$ and $c^a = bc$. Then we have that $M = \langle a, b, c, u, v, z \rangle$, where

$$\begin{array}{llllll} a^3 = I_3, & & & & & \\ b^a = c, & b^2 = c^2, & & & & \\ c^a = bc, & c^b = c^3, & c^4 = I_3, & & & \\ u^a = uv^2, & u^b = uv, & u^c = \varepsilon^2 u^2 v, & u^3 = I_3, & & \\ v^a = v, & v^b = \varepsilon^2 uv^2, & v^c = \varepsilon^2 uv, & v^u = \varepsilon v, & v^3 = I_3, & \\ z^a = z, & z^b = z, & z^c = z, & z^u = z, & z^v = z, & z^{p^k-1} = I_3. \end{array}$$

This yields a polycyclic presentation for $M$ (after replacing $\varepsilon$ by $z^{(p^k-1)/3}$). From this presentation we see that

$$\begin{aligned} M &= \langle z \rangle \, \Upsilon \, \langle a, b, c, u, v \rangle \\ &\cong C_{p^k-1} \, \Upsilon \, (E \rtimes Sp(2,3)). \end{aligned}$$

We also have that

$$M \cap SL(3, \mathbb{F}) = \begin{cases} \langle \varepsilon^{-1/3} a, b, c, u, v \rangle & \text{if } p^k \equiv 1 \bmod 9, \\ \langle b, c, u, v \rangle & \text{if } p^k \not\equiv 1 \bmod 9. \end{cases}$$

Finally, we investigate the action of field automorphisms on $M$.

**6.5.1 Theorem.** *Every automorphism of* $\mathbb{F}$*, acting entry-wise on the elements of* $M$*, normalises* $M$*.*

**Proof.** Let $\theta$ be an automorphism of $\mathbb{F}$. By looking at the entries of the matrices in our generating set for $M$, it is clear that the effect of $\theta$ on $M$ is determined by $\varepsilon\theta$. If $\varepsilon\theta = \varepsilon$, then $a$, $b$, $c$, $u$ and $v$ are fixed by $\theta$ (and $z$ is of course mapped to some power of itself), and so $\theta$ normalises $M$. If $\varepsilon\theta = \varepsilon^2$, then some calculations show that

$$a\theta = a^2,\ b\theta = c^3,\ c\theta = bc^2,\ u\theta = u \ \text{ and } \ v\theta = v^2\,.$$

Again, $\theta$ normalises $M$. ∎

# Chapter 7

# The imprimitive soluble subgroups of $GL(4,2)$ and $GL(4,3)$

## 7.1 The JS-imprimitives of $GL(4,p^k)$

Recall from Chapter 5 that we number the JS-maximals of $GL(2,p^k)$ as follows:

$$\begin{aligned}
M_1(2,p^k) &:= GL(1,p^k) \operatorname{wr} S_2\,, && p^k \neq 2\,,\\
M_2(2,p^k) &:= C_{p^{2k}-1} \rtimes C_2\,,\\
M_3(2,p^k) &:= (C_{p^k-1} \curlyvee Q_8) \dashv O^-(2,2)\,, && p^k \equiv 3 \bmod 4\,,\\
M_4(2,p^k) &:= (C_{p^k-1} \curlyvee Q_8) \dashv Sp(2,2)\,, && p^k \equiv 1 \bmod 4\,.
\end{aligned}$$

The JS-imprimitives of $GL(4,p^k)$ are listed below.

$$\begin{aligned}
M_1(4,p^k) &:= GL(1,p^k) \operatorname{wr} S_4\,, && p^k \neq 2\,,\\
M_2(4,p^k) &:= M_2(2,p^k) \operatorname{wr} S_2\,,\\
M_3(4,p^k) &:= M_3(2,p^k) \operatorname{wr} S_2\,, && p^k \equiv 3 \bmod 4\,,\\
M_4(4,p^k) &:= M_4(2,p^k) \operatorname{wr} S_2\,, && p^k \equiv 1 \bmod 4\,.
\end{aligned}$$

In contrast to the JS-imprimitive of prime degree, not even the base group of any of these four groups seems to admit a straight-forward analysis. In respect of the first group, the 2-subgroup structure of $GL(1,p^k) \operatorname{wr} (C_2 \times C_2)$ needs to be understood; it requires only a little thought to see what a complicated lattice is involved here. On the other hand, each of the other three groups has the advantage that there is very little wreathing action, but the disadvantage that

the base group is non-abelian. We do not attempt a general analysis of any of these groups. Instead, we find the imprimitive soluble subgroups of $GL(4,2)$ by an easy theoretical argument, and those of $GL(4,3)$ by making extensive use of CAYLEY. The JS-primitives of $GL(4,p^k)$ permit a more general discussion, and so are treated in a separate chapter (Chapter 8).

## 7.2 The imprimitive soluble subgroups of $GL(4,2)$

There is one JS-imprimitive of $GL(4,2)$, namely

$$M_2 := GL(2,2) \operatorname{wr} S_2 .$$

A polycyclic presentation for $M_2$ is:

$$\begin{aligned} \{ a,b,c,d,e \mid\ & a^2 = 1, \\ & b^a = d, \quad b^2 = 1, \\ & c^a = e, \quad c^b = c^2, \quad c^3 = 1, \\ & d^a = b, \quad d^b = d, \quad d^c = d, \quad d^2 = 1, \\ & e^a = c, \quad e^b = e, \quad e^c = e, \quad e^d = e^2, \quad e^3 = 1 \} . \end{aligned}$$

We do not write down the matrices referred to in this presentation, as it is obvious what they are.

**7.2.1 Theorem.** *A complete and irredundant list of $GL(4,2)$-conjugacy class representatives of the irreducible subgroups of $M_2$ is:*

$$\langle a,b,c,d,e \rangle, \langle ab,c,e \rangle, \langle a,bd,c,e \rangle, \langle a,c,e \rangle .$$

**Proof.** Let $G$ be an irreducible subgroup of $M_2$. Since $M_2$ has order $2^3 3^2$ and we are in characteristic 2, it follows that $G$ is not a 2-group. So the Sylow 3-subgroups of $G$ have order 3 or 9. Suppose that the Sylow 3-subgroups of $G$ have order 3. Then $G$ meets the base group of $M_2$ in a subgroup of order 3, 6 or 12 (which is normal in $G$), and $G$ has order 6, 12 or 24, respectively. Every group of order 12 has a non-trivial characteristic 2-subgroup, and therefore $G$ cannot have order 12 or 24. Clearly $G$ cannot be $C_6$, and since every faithful irreducible representation

of $S_3$ over $GF(2)$ has degree 2, $G$ cannot be $S_3$ either. Therefore $G$ contains the unique Sylow 3-subgroup of $M_2$. So we seek those subgroups of $M_2$ which contain $\langle c, e \rangle$ and which are not subgroups of the base group, $\langle b, c, d, e \rangle$. Since the quotient of $M_2$ by $\langle c, e \rangle$ is $D_8$, it is not difficult to see that the subgroups of $M_2$ which satisfy these requirements are those listed in the theorem, plus $\langle abd, c, e \rangle$; this group is conjugate in $M_2$ to $\langle a, c, e \rangle$, and so need not be considered. The four groups listed in the theorem are pairwise non-isomorphic, and so all that remains to do is show that they are irreducible. Since each contains the third and/or fourth group listed, it suffices to establish the irreducibility of those two groups. This follows easily from the fact that the natural module for $\langle c, e \rangle$ is the direct sum of two non-isomorphic irreducible submodules which are interchanged by $a$. ■

## 7.3 Computing the imprimitive soluble subgroups of $GL(4,3)$

In this section we outline an algorithm for finding one representative from each $GL(4,3)$-conjugacy class of imprimitive soluble subgroups. This algorithm is discussed with reference to CAYLEY, in which it has been implemented. A brief description of CAYLEY is given in Section 1.2, and the notation we use for its features can be found in Section 1.3. The code for some of the CAYLEY procedures mentioned below is listed in Appendix C.

Before describing the algorithm, we give some details of the procedure `ISOTEST`, as we use this procedure frequently in this and the next two chapters. `ISOTEST` takes as input a group, whose order it then calculates. If this order is sufficiently 'small' (to be explained below), then `ISOTEST` calculates as many invariants of the group as are needed to distinguish it from all other groups of that same order. Then the group is assigned an identifier (which consists of a number and, where possible, a meaningful name) and this information is returned. (Actually, some groups are so difficult to distinguish that the identifier passed back can refer to a family of groups rather than a single group.) `ISOTEST` deals with groups of the

following orders:

1. any order that is the product of three or fewer primes;

2. order $8q$, where $q$ is an odd prime;

3. order $p^2q^2$, where $p$ and $q$ are distinct primes;

4. orders 16, 32, 48, 64 and 81.

ISOTEST is based on the procedure ISOMTEST in the CAYLEY library TWOGPS of Newman and O'Brien (1989). That procedure deals with the groups whose order divides 64 (but does not assign names to them), and for these groups we use the numbering provided by the TWOGPS library. For the orders dividing 81, I use the numbering of a 3-groups library developed by Baldwin (1987). For order 48, I use the numbering of Neubüser (1967). For the groups of the other orders listed above, I use my own numbering. (The groups of these orders have been determined in the literature, but I carried out an independent determination—my numbering reflects the way in which I did this.) The format for the numbering of a group is its order, followed by a symbol (usually #), followed by some numbers and possibly some letters. For example, 8#3 is the identifier of $D_8$. Note that we use the numeric identifier in the text only when ISOTEST does not provide a name for the group.

**7.3.1 Remark.** ISOTEST will be used implicitly in many places in this and the next two chapters. If no justification is given for a claim about the isomorphism type of a group, or for a claim that several groups are pairwise non-isomorphic, then that claim is proved by applying ISOTEST.

Now we describe an algorithm for obtaining a complete and irredundant set of $GL(4,3)$-conjugacy class representatives of the imprimitive soluble subgroups of $GL(4,3)$.

1. Every imprimitive soluble subgroup of $GL(4,3)$ is conjugate to a subgroup of $M_1$, $M_2$ or $M_3$. So it is only necessary to examine the subgroups of these

three groups. Note that $M_1$ is monomial whereas the other two are not, and that $M_2$ is a Sylow 2-subgroup of $GL(4,3)$. Let $M$ be one of $M_1$, $M_2$ or $M_3$. Write down a polycyclic presentation for $M$ as abstract group, and input this to CAYLEY.

2. We invoke the CAYLEY function lattice on $M$. The output, `lat` say, of this function is a sequence of subgroups of $M$ with the property that every subgroup of $M$ is conjugate to exactly one member of `lat`. A generating set is also stored for each member of `lat`.

3. At this point we require an explicit isomorphism $\varphi$ from (the finitely presented) $M$ to an irreducible subgroup of $GL(4,3)$. The procedure `GETIRR` finds all members of `lat` whose image under $\varphi$ is irreducible and places them in a set, `irred` say.

4. `Irred` is a complete and irredundant set of $M$-conjugacy class representatives of the irreducible subgroups of $M$. We now partition `irred` into two sets, `keep` and `throw`. When the algorithm terminates, `keep` will be a complete and irredundant set of representatives of the $GL(4,3)$-conjugacy classes of imprimitive soluble subgroups whose guardian is $M$.

5. We have to transfer to `throw` each member of `irred` whose guardian is not $M$. An imprimitive soluble subgroup of $GL(4,3)$ whose guardian is $M_1$ can be recognised because $M_1$ is monomial: when $M$ is $M_2$ or $M_3$, we use the procedure `RIDMON` to transfer the monomial groups in `irred` to `throw`. A subgroup of $GL(4,3)$ whose guardian is $M_2$ can be recognised because $M_2$ is a Sylow 2-subgroup of $GL(4,3)$: when $M = M_3$, we transfer the 2-groups of `irred` to `throw`.

6. Now every member of `irred` has $M$ as its guardian. If two or more members of `irred` are $GL(4,3)$-conjugate, then we transfer one of them to `keep` and the rest to `throw`. If a member of `irred` is not $GL(4,3)$-conjugate to any other member of `irred`, then we transfer this group to `keep`. We use a variety of theoretical and computational techniques to deal with these two

possibilities. At the completion of this step, `keep` has the desired properties, and the algorithm terminates.

## 7.4 The irreducible subgroups of $M_1(4,3)$

Recall that $M_1 = GL(1,3)\,\mathrm{wr}\,S_4$ and has order $2^7 3$. `GETIRR` returns a complete and irredundant set `irred` of $M_1$-conjugacy class representatives of the irreducible subgroups of $M_1$; `irred` contains 22 groups, and we must now partition it into `keep` and `throw`.

The orders of the 22 groups in `irred` are as follows: three have order 16, seven have order 32, six have order 64, one has order 96, one has order 128, three have order 192 and one has order 384. The three groups of order 16 are pairwise non-isomorphic, and so we place them in `keep`. Of the seven groups of order 32 there are five distinct isomorphism types, the only duplications being the occurrence of three groups isomorphic to 32#6.

**7.4.1 Proposition.** *Let $\mathbb{F}$ be the field of 3 elements and let $G$ be the group 32#6. Then there is exactly one isomorphism type of 4-dimensional faithful irreducible $\mathbb{F}G$-module.*

**Proof.** There are two pieces of structural information we need about $G$. The first is that it has an elementary abelian normal subgroup of order 8 (the Frattini subgroup), $H$ say, and the second is that its centre has order 2. By Theorem 3.2.5, $Z(G)$ is the unique minimal normal subgroup of $G$. In particular, $Z(G) \leq H$. Observe that $H$ has seven maximal subgroups, and exactly three of them contain $Z(G)$. Because $Z(G)$ is the unique minimal normal subgroup of $G$, the other four maximal subgroups of $H$ must lie in a single $G$-conjugacy class.

Let $U$ be a 4-dimensional faithful irreducible $\mathbb{F}G$-module (such a module exists because we have explicitly found one above). By Clifford's Theorem, $U|_H$ is the direct sum of $G$-conjugate irreducible $\mathbb{F}H$-modules. The irreducible $\mathbb{F}H$-modules are of course 1-dimensional, and so $U|_H$ is the direct sum of four 1-dimensional $G$-conjugate $\mathbb{F}H$-modules, say $U_H = V_1 \oplus \ldots \oplus V_4$. Since $\mathrm{Hom}_{\mathbb{F}H}(U|_H, V_i) \neq 0$, we have by Nakayama's Lemma that $\mathrm{Hom}_{\mathbb{F}G}(U, V_i^G) \neq 0$. Since $V_i^G$ has dimension 4,

we conclude that $U \cong V_i^G$. The kernels of the $V_i$ are $G$-conjugate subgroups of $H$, which must intersect trivially because $U$ is faithful. As the quotient of $H$ by any such kernel is cyclic, the kernels cannot have order 2; hence they must be exactly the four maximal subgroups of $H$ which do not contain $Z(G)$. This proves our claim. ■

Therefore we place two of the groups of `irred` isomorphic to 32#6 in `throw` and the other five groups of order 32 in `keep`. Now consider the six groups of order 64 in `irred`. There are exactly four distinct isomorphism types among them. There are two groups isomorphic to $C_2 \,\mathrm{wr}\, (C_2 \times C_2)$ and two groups isomorphic to $C_2 \,\mathrm{wr}\, C_4$. When we analyse the irreducible subgroups of $M_2$ in the next section we will find that there is just one irreducible subgroup of each of these two isomorphism types in $M_2$, which is a Sylow 2-subgroup of $GL(4,3)$. Therefore we place in `keep` a certain four groups of order 64 from `irred` and we place the other two in `throw`. There is only one group of each of the orders 96, 128 and 384 in `irred`, and so we put these three groups in `keep`. This leaves only the three groups of order 192, which `ISOTEST` cannot identify. However, the groups can be seen to be pairwise non-isomorphic by the isomorphism types of their Sylow 2-subgroups and the orders of their derived groups. So we put these three groups in `keep`.

Thus we have established that there are exactly 18 $GL(4,3)$-conjugacy classes of irreducible soluble subgroups whose guardian is $M_1$, and we have obtained a complete and irredundant set of representatives of these classes.

## 7.5 The irreducible subgroups of $M_2(4,3)$

Recall that $M_2 = SD_{16} \,\mathrm{wr}\, S_2$, and has order $2^9$. This is a Sylow 2-subgroup of $GL(4,3)$. `GETIRR` returns a complete and irredundant set `irred` of $M_2$-conjugacy class representatives of the irreducible subgroups of $M_2$; there are 63 such groups. `RIDMON` transfers to `throw` the monomial groups, leaving 41 in `irred`.

The six groups of order 256 in `irred` can be seen to be pairwise non-isomorphic by using `ISOTEST` on their derived groups and derived quotients. The nine groups

of order 128 in `irred` can be seen to be pairwise non-isomorphic by using `ISOTEST` on their derived groups and Frattini subgroups, and by counting their conjugacy classes of elements. This leaves us only with groups that can be identified by `ISOTEST`. The isomorphism types which are represented more than once by the groups in `irred` are: $Q_{16}$, $Q_{16} \curlyvee C_4$, 32#8, 32#44, 64#37 and 64#137. By looking at the irreducible subgroups of $M_3$, we find a single $M_3$-conjugacy class of 32#8, 64#37, and 64#137, so that eliminates three cases.

**7.5.1 Proposition.** *Let $\mathbb{F}$ be the field of 3 elements, and let $G$ be the group $Q_{16}$. Then there is exactly one isomorphism type of faithful irreducible $\mathbb{F}G$-module, and it has dimension 4.*

**Proof.** Let $U$ be a 4-dimensional faithful irreducible $\mathbb{F}G$-module (such a module exists because we have explicitly found one above). The endomorphism algebra of $U$ cannot have $\mathbb{F}$-dimension 4 because the Singer cycles are self-centralising, and it cannot have $\mathbb{F}$-dimension 1 because absolutely irreducible groups of prime power order are monomial. Therefore there are exactly two copies of $U$ in any direct decomposition of $\mathrm{Reg}(\mathbb{F}G)$. The centre of $G$ is the unique minimal normal subgroup of $G$, and $G/Z(G)$ has order 8. It now follows that

$$\mathrm{Reg}(\mathbb{F}G) \cong \mathrm{Reg}(\mathbb{F}(G/Z(G))) \oplus U \oplus U\,. \quad \blacksquare$$

**7.5.2 Proposition.** *The irreducible subgroups of $GL(4,3)$ that are isomorphic to $Q_{16} \curlyvee C_4$ lie in a single conjugacy class.*

**Proof.** Denote $GL(4,3)$ by $L$. Let $G_1$ and $G_2$ be irreducible subgroups of $L$ that are isomorphic to $Q_{16} \curlyvee C_4$, and let $H_1$ and $H_2$ be subgroups of $G_1$ and $G_2$, respectively, that are isomorphic to $Q_{16}$. Since $H_i$ is monolithic and completely reducible, the previous proposition shows that $H_i$ is irreducible. Therefore $H_1$ and $H_2$ are $L$-conjugate. Since $H_i$ is irreducible, we have that $\mathbf{C}_L(H_i)$ is cyclic, and so contains a unique cyclic subgroup of order 4, which of course is $\mathbf{C}_{G_i}(H_i)$. Since $G_i = H_i\mathbf{C}_{G_i}(H_i)$, it follows that any matrix which conjugates $H_1$ to $H_2$ must also conjugate $G_1$ to $G_2$. $\blacksquare$

**7.5.3 Lemma.** *Let* $\mathbb{F}$ *be the field of* 3 *elements, and let* $G$ *be a monolithic group containing a subgroup* $H$ *that is cyclic of order* 8 *in which all four elements of order* 8 *are* $G$*-conjugate. Then every* 4*-dimensional faithful irreducible* $\mathbb{F}G$*-module is absolutely irreducible.*

**Proof.** Suppose that $U$ is a faithful irreducible $\mathbb{E}G$-module, where $\mathbb{E}$ is an algebraically closed field containing $\mathbb{F}$. Let $c$ be an element of $H$ of order 8. In $G$ the elements $c$, $c^3$, $c^5$ and $c^7$ are pairwise conjugate. Therefore the matrix representing the action of $c$ on $U$ has at least four distinct eigenvalues, implying that $\dim(U) \geq 4$. Since $G$ is monolithic, it now follows that every 4-dimensional faithful irreducible $\mathbb{F}G$-module is absolutely irreducible. ∎

**7.5.4 Proposition.** *Let* $\mathbb{F}$ *be the field of* 3 *elements, and let* $G$ *be the group* 32#44*. Then there is exactly one isomorphism type of faithful irreducible* $\mathbb{F}G$*-module, and it has dimension* 4*.*

**Proof.** Let $U$ be a 4-dimensional faithful irreducible $\mathbb{F}G$-module (such a module exists because we have explicitly found one above). Since $G$ contains a self-centralising normal subgroup isomorphic to $C_8$, we see that the four elements of order 8 in this subgroup are $G$-conjugate. The centre of $G$ has order 2 and so is the unique minimal normal subgroup of $G$. Then by Lemma 7.5.3, $U$ is absolutely irreducible. It now follows that

$$\mathrm{Reg}(\mathbb{F}G) \cong \mathrm{Reg}(\mathbb{F}(G/Z(G))) \oplus U \oplus U \oplus U \oplus U\,. \quad ∎$$

Using the above propositions, we transfer eight of the 41 groups in `irred` to `throw`, and transfer the other 33 to `keep`.

Thus we have established that there are exactly 33 $GL(4,3)$-conjugacy classes of irreducible soluble subgroups whose guardian is $M_2$, and we have obtained a complete and irredundant set of representatives of these classes.

## 7.6 The irreducible subgroups of $M_3(4,3)$

Recall that $M_3 = GL(2,3)\,\mathrm{wr}\,S_2$ and has order $2^9 3^2$. `GETIRR` returns a complete and irredundant set `irred` of $M_3$-conjugacy class representatives of the irreducible

subgroups of $M_3$; there are 70 groups in `irred`. Transfering the 2-groups of `irred` to `throw` leaves just 15. Using `RIDMON` shows that none of these are monomial. So the 15 groups left in `irred` are not conjugate to subgroups of $M_1$ or $M_2$.

Of the 15 groups in `irred`, two have order 48, five have order 96, one has order 192, two have order 384, one has order 768, one has order 1152, two have order 2304, and one has order 4608. `ISOTEST` shows that the two groups of order 48 are not isomorphic. So the only orders for which there may be $GL(4,3)$-conjugate groups in `irred` are 96, 384 and 2304. The two groups of order 2304 cannot be conjugate because their derived quotients are not isomorphic. The two groups of order 384 cannot be conjugate because their derived groups have different orders. Using `ISOTEST` on the Sylow 2-subgroups of the five groups of order 96, we find four isomorphism types. Hence we are left with just two groups of order 96 to discuss. In fact these two are $GL(4,3)$-conjugate, as we now prove.

**7.6.1 Lemma.** *The two remaining groups of order* 96 *in* `irred` *are isomorphic.*

**Proof.** Using CAYLEY we find that each of the two groups has a normal $GL(2,3)$ which is complemented by a $C_2$, and that this $C_2$ centralises the $SL(2,3)$ in $GL(2,3)$, but does not centralise the $GL(2,3)$. Let $G$ be any group with these properties. Then we can write $G = \langle a, b, S\rangle$, where $S \cong SL(2,3)$, $b$ has order 2, $\langle b, S\rangle \cong GL(2,3)$, $a$ has order 2, $b^a \neq b$, and $a$ centralises $S$. So $b^a = bs$, for some non-trivial $s \in S$. It follows that $s$ has order 2. Since $S$ contains a unique element of order 2, we see that there is exactly one group of order 96 with these properties. Therefore the two groups in question are isomorphic. ∎

**7.6.2 Lemma.** *The two remaining groups of order* 96 *in* `irred` *are* $GL(4,3)$*-conjugate.*

**Proof.** Let $\mathbb{F}$ be the field of 3 elements, let $G$ be a group isomorphic to one of these groups, and let $H$ be its unique subgroup isomorphic to $GL(2,3)$. Let $U$ be a 4-dimensional faithful irreducible $\mathbb{F}G$-module (such a module exists because we have explicitly found one above). The centre of $G$ has order 2 and is the unique minimal normal subgroup of $G$. Also, $G$ contains a cyclic subgroup

of order 8 in which all four elements of order 8 are conjugate. Therefore, by Lemma 7.5.3, $U$ is absolutely irreducible. By Clifford's Theorem, $U|_H$ is the direct sum of $G$-conjugate irreducible $\mathbb{F}H$-modules. Every normal subgroup of $H$ is characteristic in $H$ and so normal in $G$. Since $U$ is faithful, $U|_H$ is a direct sum of faithful irreducible $\mathbb{F}H$-modules. By Huppert and Blackburn (1982, Exercise VII.3.4, p. 43) there are exactly two such modules, each of dimension 2. So $U|_H = V_1 \oplus V_2$, where the $V_i$ are faithful irreducible $\mathbb{F}H$-modules. Since $U$ is absolutely irreducible, it follows from Nakayama's Lemma that $V_1 \ncong V_2$. Also by Nakayama's Lemma, $U \cong V_i^G$. Hence there is just one isomorphism type of 4-dimensional faithful irreducible $\mathbb{F}G$-module, and this shows that our two groups of order 96 are conjugate in $GL(4,3)$. ■

Thus we have established that there are exactly 14 $GL(4,3)$-conjugacy classes of irreducible soluble subgroups whose guardian is $M_3$, and we have obtained a complete and irredundant set of representatives of these classes.

## 7.7 Summary

There are 65 $GL(4,3)$-conjugacy classes of imprimitive soluble subgroups. We have picked exactly one representative from each of these classes. Table 7.1 details how many groups of each order there are in this set of representatives.

| order | number | order | number |
|---|---|---|---|
| 16 | 5 | 256 | 6 |
| 32 | 12 | 384 | 3 |
| 48 | 2 | 512 | 1 |
| 64 | 12 | 768 | 1 |
| 96 | 5 | 1152 | 1 |
| 128 | 10 | 2304 | 2 |
| 192 | 4 | 4608 | 1 |

Table 7.1: The imprimitive soluble subgroups of $GL(4,3)$

# Chapter 8

# The primitive soluble subgroups of $GL(4, p^k)$

## 8.1 The JS-primitives of $GL(4, p^k)$

There is one JS-primitive of $GL(4, p^k)$ whose unique maximal abelian normal subgroup has order $p^{4k} - 1$, namely

$$M_5(4, p^k) := C_{p^{4k}-1} \rtimes C_4 ,$$

the normaliser of a Singer cycle.

There is one JS-primitive of $GL(4, p^k)$ whose unique maximal abelian normal subgroup has order $p^{2k} - 1$, namely

$$M_6(4, p^k) := M_4(2, p^{2k}) \rtimes C_2 , \quad p \neq 2 .$$

As described in Section 2.5, we think of the field of $p^{2k}$ elements here as the field of 2 by 2 matrices that is the linear span of our fixed Singer cycle of $GL(2, p^k)$.

Now we come to the JS-primitives of $GL(4, p^k)$ whose unique maximal abelian normal subgroup is the scalar group. Let $M$ be such a group. There are three cases to examine.

**Case 1.** Assume that $p^k \equiv 3 \bmod 4$ and that the Fitting subgroup $F$ of $M$ is $C_{p^k-1} \curlyvee D_8 \curlyvee D_8$. Then $M/F$ is isomorphic to a completely reducible maximal soluble subgroup of $O^+(4, 2)$ that does not fix any non-zero isotropic subspace

of the natural module for $O^+(4,2)$. However, $O^+(4,2)$ is isomorphic to $S_3 \operatorname{wr} S_2$, so in particular it is soluble. Therefore $M/F = O^+(4,2)$. So in this case we find exactly one JS-primitive,

$$M_7(4,p^k) := (C_{p^k-1} \curlyvee D_8 \curlyvee D_8) \leftthreetimes O^+(4,2)\,.$$

**Case 2.** Assume that $p^k \equiv 3 \bmod 4$ and that the Fitting subgroup $F$ of $M$ is $C_{p^k-1} \curlyvee D_8 \curlyvee Q_8$. Then $M/F$ is isomorphic to a completely reducible maximal soluble subgroup of $O^-(4,2)$ that does not fix any non-zero isotropic subspace of the natural module for $O^-(4,2)$. It is shown in Appendix B that there is a unique $O^-(4,2)$-conjugacy class of such groups and that each group in this class is isomorphic to $\mathrm{Hol}(C_5)$. Therefore $M/F = \mathrm{Hol}(C_5)$. So in this case we find exactly one JS-primitive,

$$M_8(4,p^k) := (C_{p^k-1} \curlyvee D_8 \curlyvee Q_8) \leftthreetimes \mathrm{Hol}(C_5)\,.$$

**Case 3.** Assume that $p^k \equiv 1 \bmod 4$. Therefore we can write the Fitting subgroup $F$ of $M$ as $C_{p^k-1} \curlyvee D_8 \curlyvee D_8$. Then $M/F$ is isomorphic to a completely reducible maximal soluble subgroup of $Sp(4,2)$ that does not fix any non-zero isotropic subspace of the natural module for $Sp(4,2)$. By methods analogous to those in Appendix B it can be shown that every such subgroup is $Sp(4,2)$-conjugate to either $O^+(4,2)$ or $\mathrm{Hol}(C_5)$. So in this case we find exactly two JS-primitives,

$$\begin{aligned} M_9(4,p^k) &:= (C_{p^k-1} \curlyvee D_8 \curlyvee D_8) \leftthreetimes O^+(4,2)\,, \\ M_{10}(4,p^k) &:= (C_{p^k-1} \curlyvee D_8 \curlyvee D_8) \leftthreetimes \mathrm{Hol}(C_5)\,. \end{aligned}$$

Although $M_9(4,p^k)$ and $M_{10}(4,p^k)$ admit the same description as $M_7(4,p^k)$ and $M_8(4,p^k)$, respectively, they arise in different ways and so are given different numbers.

Jordan (see Appendix A) claims that there are five conjugacy classes of maximal irreducible soluble subgroups of $GL(4,3)$, but there are only four. The JS-maximals of $GL(4,3)$ are $M_1$, $M_2$, $M_3$, $M_5$, $M_6$, $M_7$ and $M_8$. Of these, $M_3$, $M_5$, $M_7$ and $M_8$ are maximal soluble, while $M_1$ and $M_6$ are conjugate to subgroups of $M_7$, and $M_2$ is a conjugate to a subgroup of $M_3$.

## 8.2 A generating set for $M_6(4, p^k)$

Recall that $M_6 = M_4(2, p^{2k}) \rtimes C_2$. We already have a polycyclic presentation for $M_4(2, p^{2k})$. From the proof of Theorem 5.2.2, we see that an extra element of order 2 needed to generate $M_6(4, p^k)$ can be chosen so that it acts $p$-th poweringly on a generator of the centre of $M_4(2, p^{2k})$, and trivially on each of the other members of our canonical generating set for $M_4(2, p^{2k})$. This suggests the next result.

**8.2.1 Proposition.** *$M_6(4, p^k) = M_2(2, p^k) \otimes M_i(2, p^k)$, where $i$ is 3 or 4 according as $p^k$ is congruent to 3 or 1 modulo 4, respectively.*

**Proof.** Set $G := M_2(2, p^k) \otimes M_i(2, p^k)$. Then $|G| = 48(p^{2k} - 1)$. Let $A$ be our fixed Singer cycle of $GL(2, p^k)$. It is not difficult to see that $A \otimes I_2$ is the unique maximal abelian normal subgroup of both $G$ and $M_6(4, p^k)$. Therefore $G \leq \mathbf{N}_{GL(4,p^k)}(A) = M_6(4, p^k)$ (this last equality because $Sp(2, 2)$ is soluble). Since $|G| = |M_6|$, the result follows. ∎

It is now easy to write down a polycyclic presentation for $M_6(4, p^k)$.

## 8.3 A generating set for $M_7(4, p^k)$

Recall that $M_7 = (C_{p^k-1} \curlyvee D_8 \curlyvee D_8) \rtimes O^+(4, 2)$. Let $F$ be the Fitting subgroup of $M_7$. We could find a generating set for $M_7$ by the methods given in Section 2.5, but the following structure theorem yields a much simpler way.

**8.3.1 Theorem.** *$M_7$ is conjugate to $(M_3(2, p^k) \otimes M_3(2, p^k)) \rtimes S_2$, where the non-trivial element of the $S_2$ is the permutation matrix that interchanges the tensor factors.*

**Proof.** Let $G$ be the group $(M_3(2, p^k) \otimes M_3(2, p^k)) \rtimes S_2$, as defined in the statement of the theorem. Then $\mathrm{Fit}(G)$ is the tensor square of $\mathrm{Fit}(M_3(2, p^k))$, and so $\mathrm{Fit}(G) \cong C_{p^k-1} \curlyvee Q_8 \curlyvee Q_8$. Since $Q_8$ is absolutely irreducible in $GL(2, p^k)$, it follows from the Outer Tensor Product Theorem that $\mathrm{Fit}(G)$ is irreducible. Then

by Theorem 2.4.7, $\mathrm{Fit}(G)$ is conjugate to $F$. So $G$ is conjugate to a subgroup of the normaliser in $GL(4,p^k)$ of $F$, namely $M_7$. Since $|G| = |M_7|$, the result follows. ∎

We now *redefine* $M_7(4,p^k)$ to be $(M_3(2,p^k) \otimes M_3(2,p^k)) \rtimes S_2$. It is then easy to write down a polycyclic presentation for $M_7$.

Note that

$$M_7 \cong \begin{cases} C_{p^k-1} \,\mathrm{Y}\, (GL(2,3) \,\mathrm{cr}\, S_2) & \text{if } p^k \equiv 3 \bmod 8\,, \\ C_{p^k-1} \,\mathrm{Y}\, (BO \,\mathrm{cr}\, S_2) & \text{if } p^k \equiv 7 \bmod 8\,, \end{cases}$$

where by $G \,\mathrm{cr}\, T$ we mean the *crown product* of the group $G$ and the transitive permutation group $T$. In our case the crown product can be defined (abstractly) as the quotient of the wreath product by the unique diagonal central subgroup of the base group.

Obviously it is important to find the primitive subgroups of $GL(2,3) \,\mathrm{cr}\, S_2$ and $BO \,\mathrm{cr}\, S_2$. Let $N$ be either of these groups, let $A$ be the centre of $N$ (the scalar subgroup of order 2) and let $E$ be the Fitting subgroup of $N$. Then $E/A$ is a symplectic space on which $N/E$ acts in the natural way as $O^+(4,2)$. The following theorem identifies those primitive subgroups of $N$ which contain $E$.

**8.3.2 Theorem.** *Let $G$ be a subgroup of $N$ that contains $E$. Then $G$ is imprimitive if and only if $G/E$ normalises a maximal isotropic subspace of $E/A$.*

**Proof.** We know that $G$ is irreducible because $E$ is already irreducible. Suppose that $G/E$ normalises a maximal isotropic subspace of $E/A$. This subspace of $E/A$ corresponds to an abelian normal subgroup of $G$ that is not cyclic (as its quotient by $A$ is not cyclic). Consequently $G$ cannot be primitive (see Theorem 2.5.8).

Now suppose that $G$ is monomial. Let $U$ be the natural module for $G$, let $V$ be a 1-dimensional block of imprimitivity for $G$ and let $H$ be the normaliser in $G$ of $V$. Clearly $V$ is also a block of imprimitivity for $E$, and $H \cap E$ is the normaliser in $E$ of $V$. Therefore $H \cap E \geq A$, $|E\colon H \cap E| = 4$ and $U|_E \cong \mathrm{Ind}_{H\cap E}^{E}(V|_{H\cap E})$. Let $K$ be the kernel of $V|_{H\cap E}$. Since $U|_E$ is faithful, it follows that $K$ is $E$-core-free. This shows that $H \cap E$ cannot be isomorphic to $D_8$ or $Q_8$. Since $E$ has no subgroup isomorphic to $C_8$, we see that $H \cap E$ must be isomorphic to $C_4 \times C_2$

or the elementary abelian group of order 8. Each of these corresponds to a maximal isotropic subspace of $E/A$. Since $E$ is irreducible, we have that $G = HE$. Therefore $H \cap E \trianglelefteq G$, because $H \cap E \trianglelefteq E$. Consequently, $G/E$ normalises a maximal isotropic subspace of $E/A$. (Note that since $p^k \equiv 3 \bmod 4$, $H \cap E$ cannot be $C_4 \times C_2$.)

Finally, suppose that $G$ is imprimitive but not monomial. Let $U$ be the natural module for $G$, let $V$ be a 2-dimensional block of imprimitivity for $G$ and let $H$ be the normaliser in $G$ of $V$. Clearly $V$ is also a block of imprimitivity for $E$, and $H \cap E$ is the normaliser in $E$ of $V$. Therefore $H \cap E \geq A$, $|E\colon H \cap E| = 2$ and $U|_E \cong \mathrm{Ind}_{H\cap E}^{E}(V|_{H\cap E})$. Let $K$ be the kernel of $V|_{H\cap E}$. Since $U|_E$ is faithful, it follows that $K$ is $E$-core-free. Each subgroup of $E$ of index 2 is isomorphic to either $D_8 \times C_2$ or $D_8 \curlyvee C_4$. Suppose that $H \cap E \cong D_8 \curlyvee C_4$. Then $H \cap E$ is monolithic, and since $U|_E$ is faithful, it follows that $V|_{H\cap E}$ is faithful. Furthermore, $V|_{H\cap E}$ is irreducible because of Maschke's Theorem and the fact that $H \cap E$ is not abelian. So there must be an irreducible $D_8 \curlyvee C_4$ in $GL(2, p^k)$. From our knowledge of the irreducible soluble subgroups of $GL(2, p^k)$ for $p^k \equiv 3 \bmod 4$, we see that this is impossible. Therefore $H \cap E \cong D_8 \times C_2$. As in the previous case, $H \cap E \trianglelefteq G$. Observe that $D_8 \times C_2$ has a characteristic $C_4 \times C_2$, which is then normal in $G$. Again, $G/E$ normalises a maximal isotropic subspace of $E/A$ (whose preimage in $E$ is $C_4 \times C_2$). ■

The subgroups of $O^+(4,2)$ are discussed in Appendix B.

## 8.4 A generating set for $M_8(4, p^k)$

Let $\mathbb{F}$ be the field of $p^k$ elements, where $p^k \equiv 3 \bmod 4$. We construct a generating set for $M_8$ by the methods described in Section 2.5. Let $z$ be a generator for the scalar group, and define $u_1$, $v_1$, $u_2$ and $v_2$ by

$$u_1 := I_2 \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad u_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes I_2,$$

$$v_1 := I_2 \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad v_2 := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} \otimes I_2,$$

where $\alpha$ and $\beta$ belong to the prime subfield of $\mathbb{F}$, and $\alpha^2 + \beta^2 = -1$. Then $\{u_1, v_1, u_2, v_2, z\}$ generates the Fitting subgroup $F$ of $M_8$. To extend this set to a generating set for $M_8$, we first require a generating set for $\mathrm{Hol}(C_5)$. Actually, it is more convenient to choose a generating set for $O^-(4,2)$. We choose this set to consist of the three matrices $f\rho$, $g\rho$ and $h\rho$ defined below.

$$f\rho := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g\rho := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad h\rho := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

(See Appendix B for an explanation of how these matrices were found.) Setting $b\rho := h\rho f\rho$ and $a\rho := (g\rho f\rho)^2 b\rho g\rho$, we find that $a\rho$ has order 4, $b\rho$ has order 5, and $(b\rho)^{a\rho} = (b\rho)^2$, so that $\langle a\rho, b\rho \rangle \cong \mathrm{Hol}(C_5)$. There are two reasons we work with $f\rho$, $g\rho$ and $h\rho$. One reason is that each is an involution; this means that the solutions to the linear equations we must solve are less complicated. The other reason is that each of these matrices has mainly zeros in its last column; experience shows that calculations not involving $v_2$ are much simpler. It is also useful that the first three rows of $g\rho$ and $h\rho$ are the same.

By the theory in Section 2.5, there exists a matrix $f$ of $GL(4, \mathbb{F})$ such that

$$\begin{aligned} u_1^f &= \lambda_1 u_1, \\ v_1^f &= \mu_1 u_1 v_1 v_2, \\ u_2^f &= \lambda_2 u_1 u_2, \\ v_2^f &= \mu_2 v_2, \end{aligned}$$

where the $\lambda_i$ and $\mu_j$ are scalars. Setting $\lambda_1 = \lambda_2 = \mu_1 = 1$ and $\mu_2 = -1$, we find that one such matrix is

$$f := 2^{-1} \begin{pmatrix} \beta & 1-\alpha & -\beta & 1+\alpha \\ -1-\alpha & -\beta & -1+\alpha & \beta \\ -\beta & 1+\alpha & \beta & 1-\alpha \\ -1+\alpha & \beta & -1-\alpha & -\beta \end{pmatrix}.$$

Then $f$ has determinant 1, and its square is $-I_4$.

Let $\delta$ be an element of $\mathbb{F}$ such that

$$\delta^2 = \begin{cases} -2 & \text{if } p^k \equiv 3 \bmod 8\,, \\ 2 & \text{if } p^k \equiv 7 \bmod 8\,. \end{cases}$$

By the theory in Section 2.5, there exists a matrix $g$ of $GL(4,\mathbb{F})$ such that

$$\begin{aligned} u_1^g &= \lambda_1 v_1\,, \\ v_1^g &= \mu_1 u_1\,, \\ u_2^g &= \lambda_2 u_2\,, \\ v_2^g &= \mu_2 v_2\,, \end{aligned}$$

where the $\lambda_i$ and $\mu_j$ are scalars. Setting $\lambda_1 = \mu_1 = -1$ and $\lambda_2 = \mu_2 = 1$, we find that one such matrix is

$$g := \delta^{-1} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Then $g$ has determinant 1, and its square is $-I_4$ or $I_4$, according as $p^k$ is congruent to 3 or 7 modulo 8.

By the theory in Section 2.5, there exists a matrix $h$ of $GL(4,\mathbb{F})$ such that

$$\begin{aligned} u_1^h &= \lambda_1 v_1\,, \\ v_1^h &= \mu_1 u_1\,, \\ u_2^h &= \lambda_2 u_2\,, \\ v_2^h &= \mu_2 u_2 v_2\,, \end{aligned}$$

where the $\lambda_i$ and $\mu_j$ are scalars. Setting $\lambda_2 = -1$ and $\lambda_1 = \mu_1 = \mu_2 = 1$, we find that one such matrix is

$$h := 2^{-1} \begin{pmatrix} \alpha-\beta & \alpha+\beta & \alpha-\beta & \alpha+\beta \\ \alpha+\beta & -\alpha+\beta & \alpha+\beta & -\alpha+\beta \\ \alpha-\beta & \alpha+\beta & -\alpha+\beta & -\alpha-\beta \\ \alpha+\beta & -\alpha+\beta & -\alpha-\beta & \alpha-\beta \end{pmatrix}.$$

Then $h$ has determinant 1, and its square is $-I_4$.

Now set $b := hf$. Then

$$b = 2^{-1} \begin{pmatrix} -\alpha-\beta & \alpha-\beta & -\alpha-\beta & \alpha-\beta \\ \alpha-\beta & \alpha+\beta & \alpha-\beta & \alpha+\beta \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix}.$$

Also, $b$ has determinant 1 and order 5. The action of $b$ on $F$ is given by the matrix

$$b\rho = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Now set $a := (gf)^2 bg$. Then

$$a = \delta^{-3} \begin{pmatrix} 1+\alpha-\beta & 1+\alpha+\beta & -1-\alpha-\beta & 1+\alpha-\beta \\ -1+\alpha+\beta & 1-\alpha+\beta & -1+\alpha-\beta & -1+\alpha+\beta \\ -1-\alpha+\beta & -1 \mp \alpha-\beta & -1-\alpha-\beta & 1 \mp \alpha-\beta \\ 1-\alpha-\beta & -1+\alpha-\beta & -1+\alpha-\beta & -1+\alpha+\beta \end{pmatrix}.$$

Also, $a$ has determinant 1 and its fourth power is $-I_4$. Furthermore, $b^a = b^2$. The action of $a$ on $F$ is given by the matrix

$$a\rho = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Finally we have that $M_8 = \langle a, b, u_1, v_1, u_2, v_2, z \rangle$. Set $N := \langle a, b, u_1, v_1, u_2, v_2 \rangle$. It is clear that $N = M_8 \cap SL(4, \mathbb{F})$ and that $M_8 = N \curlyvee \langle z \rangle$. The given elements, without $z$, form a polycyclic generating sequence for $N$, and the corresponding

relations are:

$$
\begin{array}{llllll}
a^4 = -I_4, & & & & & \\
b^a = b^2, & b^5 = I_4, & & & & \\
u_1^a = -v_1, & u_1^b = u_1v_1v_2, & u_1^2 = I_4, & & & \\
v_1^a = u_1v_1u_2, & v_1^b = u_1, & v_1^{u_1} = -v_1, & v_1^2 = I_4, & & \\
u_2^a = -v_1v_2, & u_2^b = -u_1u_2, & u_2^{u_1} = u_2, & u_2^{v_1} = u_2, & u_2^2 = -I_4, & \\
v_2^a = v_1u_2v_2, & v_2^b = -u_1u_2v_2, & v_2^{u_1} = v_2, & v_2^{v_1} = v_2, & v_2^{u_2} = -v_2, & v_2^2 = -I_4\,.
\end{array}
$$

Note that each of these relations is independent of the value of $p^k$ modulo 8. It can be checked via CAYLEY that $N$ does not split over $N \cap F$.

## 8.5 The primitive subgroups of $M_5(4,2)$ and $M_5(4,3)$

Recall that $M_5(4,p^k) = C_{p^{4k}-1} \rtimes C_4$, the normaliser of a Singer cycle. A polycyclic presentation for $M_5$ is

$$
\begin{array}{lll}
\langle\, a, b & \mid & a^4 = 1, \\
 & & b^a = b^{p^k},\ \ b^{p^{4k}-1} = 1\,\rangle\,.
\end{array}
$$

This group has a rather simple structure. By applying the methods of Chapter 4 to this group it should be reasonably straight-forward to obtain a complete and irredundant list of its primitive subgroups. Instead of giving a general treatment, we concentrate on the cases of direct relevance to the thesis, that is, when $p^k$ is 2 or 3.

**8.5.1 Theorem.** *A complete and irredundant list of $GL(4,2)$-conjugacy class representatives of the primitive subgroups of $M_5(4,2)$ is:*

$$\langle a, b\rangle,\ \langle a^2, b\rangle,\ \langle a, b^3\rangle,\ \langle a^2, b^3\rangle,\ \langle b\rangle,\ \langle b^3\rangle\,.$$

**Proof.** Set $M := M_5(4,2)$. Note that $M$ has order 60. Clearly $\langle a, b^5\rangle$ is a Hall $\{2,3\}$-subgroup of $M$, and so all subgroups of $M$ of order prime to 5 are conjugate in $M$ to a subgroup of $\langle a, b^5\rangle$. Since $\langle a^2\rangle$ is a non-trivial normal 2-subgroup of that group, we conclude that all $5'$-subgroups of $M$ are reducible. Let $G$ be a primitive subgroup of $M$. Then $G$ contains the unique Sylow 5-subgroup of $M$.

This Sylow 5-subgroup is certainly irreducible, and is also primitive, because it has no proper subgroup of index dividing 4. So we seek those subgroups of $M$ that contain $\langle b^3 \rangle$. Since the quotient of $M$ by $\langle b^3 \rangle$ is $I_3^4$, it is not difficult to see that the subgroups of $M$ which satisfy these requirements are those listed in the theorem, plus $\langle ab^5, b^3 \rangle$ and $\langle ab^{10}, b^3 \rangle$; both of these are conjugate in $M$ to $\langle a, b^3 \rangle$, and so need not be considered. The six groups listed in the theorem are pairwise non-isomorphic, and so no two of them can be conjugate in $GL(4,2)$. ■

**8.5.2 Theorem.** *There are exactly* 21 $GL(4,3)$*-conjugacy classes of primitive soluble subgroups that have* $M_5(4,3)$ *as their guardian.*

**Proof.** Set $M := M_5(4,3)$. To find the primitive subgroups of $M$ we use CAYLEY and methods similar to those detailed in the previous chapter. The 2-subgroups of $M$ are not primitive. We define `prim` to be the set of all members of `lat` which are not 2-groups. There are 21 such groups. `ISOTEST` shows that the groups in `prim` of order dividing 40 are pairwise non-isomorphic. There are nine groups in `prim` whose order does not divide 40: five have order 80, three have order 160, and one has order 320. All of these differ in their Sylow 2-subgroups, except two groups of order 80. However, these are not isomorphic, because one is cyclic and the other is not. So we have established that there are exactly 21 $GL(4,3)$-conjugacy classes of primitive soluble subgroups that have $M_5(4,3)$ as their guardian, and we have obtained a complete and irredundant set of representatives of these classes. ■

## 8.6 Some primitive subgroups of $M_6(4,p^k)$

Recall that $M_6(4,p^k) = M_2(2,p^k) \otimes M_i(2,p^k)$, where $i$ is 3 or 4, according as $p^k$ is congruent to 3 or 1 modulo 4, respectively. Also recall that

$$M_i(2,p^k) \;\cong\; C_{p^k-1} \,Y \begin{cases} BO & \text{if } p^k \equiv \pm 1 \bmod 8\,, \\ GL(2,3) & \text{if } p^k \equiv 3 \bmod 8\,, \\ NS & \text{if } p^k \equiv 5 \bmod 8\,. \end{cases}$$

Therefore, since the scalar group is the subgroup that is amalgamated in the tensor product, we may write

$$M_6(4,p^k) \cong (C_{p^{2k}-1} \rtimes C_2) \Upsilon \begin{cases} BO & \text{if } p^k \equiv \pm 1 \bmod 8, \\ GL(2,3) & \text{if } p^k \equiv 3 \bmod 8, \\ NS & \text{if } p^k \equiv 5 \bmod 8. \end{cases}$$

The subgroup amalgamated in this central product is of order 2, except when $p^k \equiv 5 \bmod 8$, in which case it has order 4. In this central decomposition of $M_6$, denote the first central factor by $X$ and the second by $Y$. In this section we determine some primitive subgroups of $M_6(4,p^k)$ by using our knowledge of $X$, $Y$, and of the subgroups of central products (see Theorem 3.2.2).

**8.6.1 Proposition.** *Every primitive subgroup of $M_6(4,p^k)$ contains the scalar matrix $-I_4$.*

**Proof.** The proof when $p^k \equiv \pm 1 \bmod 8$ is sufficient to indicate the method. Let $G$ be a subgroup of $M_6(4,p^k)$ that does not contain $-I_4$. By examining the Burnside lattice of $BO$ in Figure 5.2, we see that $G \cap Y$ must be of order 1 or 3. Therefore $G \leq X \otimes C_6$. Observe that $X \otimes C_6 \cong X \times C_3$. If $p = 3$, then this group is reducible, and if $p \neq 3$, then it is not primitive, because it has a non-cyclic abelian normal 3-subgroup. ■

We now specialise to the case $p^k \equiv 3 \bmod 8$. Then $Y \cong GL(2,3)$. Let $G$ be a primitive subgroup of $M_6(4,p^k)$. Then $G \geq X \cap Y$, and so by Theorem 3.2.2, we can parametrise $G$ by the triple $(X_1/X_0, Y_1/Y_0, \theta)$, where $X_1 = X \cap GY$, $X_0 = X \cap G$, $Y_1 = XG \cap Y$, $Y_0 = G \cap Y$ and $\theta$ is an isomorphism from $X_1/X_0$ to $Y_1/Y_0$. Since $G$ is primitive, it is clear (from elementary properties of the tensor product) that both $X_1$ and $Y_1$ must be primitive. The primitive subgroups of $X$ were discussed in Chapter 4, and the primitive subgroups of $Y$ were discussed in Chapter 5.

**8.6.2 Lemma.** *The only possibilities for the pair $(Y_1, Y_0)$ are $(GL(2,3), GL(2,3))$, $(GL(2,3), SL(2,3))$, $(GL(2,3), Q_8)$, $(SL(2,3), SL(2,3))$ and $(SL(2,3), Q_8)$.*

**Proof.** Refer to Figure 5.1 for the Burnside lattice of $GL(2,3)$. If $Y_1$ did not contain $SL(2,3)$, then $G$ would be a subgroup of $X \otimes SD_{16}$ or $X \otimes D_{12}$. The first of these obviously has a non-cyclic abelian normal 2-subgroup and so cannot be primitive. If $p = 3$, then $X \otimes D_{12}$ is reducible, and if $p \neq 3$, then $3 \mid (p^{2k} - 1)$ and so $X \otimes D_{12}$ cannot be primitive, because it has a non-cyclic abelian normal 3-subgroup. Hence $Y_1 \geq SL(2,3)$. Since $X$ is metacyclic, it follows that $X_1/X_0$ is metacyclic. Therefore $Y_1/Y_0$ must be metacyclic too. ∎

**8.6.3 Theorem.** *Let $G$ be a subgroup of $M_6$ such that $G \cap Y \geq SL(2,3)$. If $B$ is an abelian normal subgroup of $G$, then $B \leq X$.*

**Proof.** Without loss of generality we can assume that $B \geq \langle -I_4 \rangle$. Clearly $B \cap Y$ is an abelian normal subgroup of $G \cap Y$, which is $SL(2,3)$ or $GL(2,3)$. Therefore $B \cap Y = \langle -I_4 \rangle$. Also, $G \cap Y$ must normalise $XB \cap Y$. The only subgroups of $GL(2,3)$ that are normalised by $SL(2,3)$ are the normal subgroups of $GL(2,3)$. Since $B$ is abelian, we conclude that $XB \cap Y$ is $\langle -I_4 \rangle$ or $Q_8$. Since $B$ is normal in $G$, we have from Theorem 3.2.2 that

$$(X \cap BY)/(X \cap B) \cong_\Omega (XB \cap Y)/(B \cap Y),$$

where $\Omega$ is the set of automorphisms of $X \otimes Y$ induced by the elements of $G$ acting by conjugation. Since the 3-elements of $SL(2,3)$ act trivially on $X$ but non-trivially on $Q_8/\langle -I_4 \rangle$, we conclude that $B$ cannot be a diagonal subgroup of $X \otimes Y$, and thus $B \leq X$. ∎

**8.6.4 Theorem.** *If $X_1$ is a primitive subgroup of $X$, then $X_1 \otimes SL(2,3)$ is a primitive subgroup of $M_6$.*

**Proof.** Set $G := X_1 \otimes SL(2,3)$. Let $U$ be the natural module for $G$, and suppose that $U$ is not primitive. Since $X_1$ is irreducible and $SL(2,3)$ is absolutely irreducible, it follows from the Outer Tensor Product Theorem that $G$ is irreducible. Therefore $G$ is imprimitive. Suppose that $U$ is induced from a 2-dimensional module for a subgroup $H$ of index 2. Then $H \trianglelefteq G$. Refer to Figure 8.1. Since $SL(2,3)$ has no subgroup of index 2, we conclude that $H \geq I_2 \otimes SL(2,3)$. Therefore we

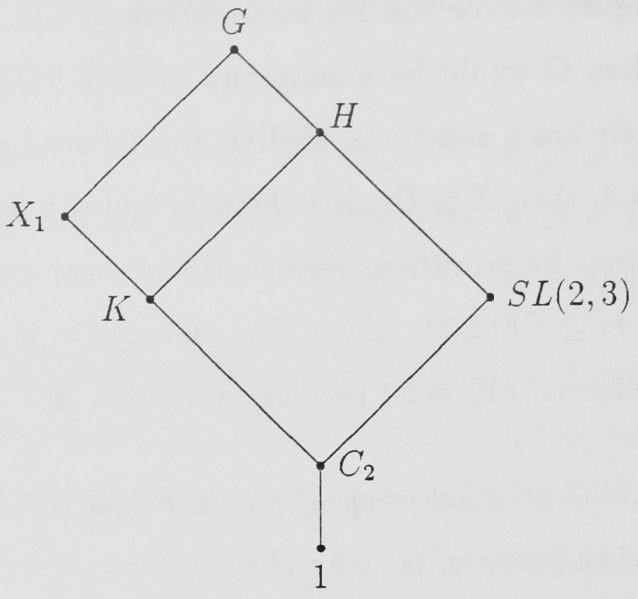



Figure 8.1: First case in Theorem 8.6.4

may write $H = K \otimes SL(2,3)$, where $\langle -I_2 \rangle \leq K \leq X_1$. Since $X_1$ is primitive and $K \trianglelefteq X_1$, it follows that $K$ is completely reducible and homogeneous. If $K$ were irreducible, then by the Outer Tensor Product Theorem, $K \otimes SL(2,3)$ would be irreducible, contradicting the reducibility of $H$. Therefore $K$ is reducible. Since the degree of $K$ is prime, we conclude that $K$ is scalar. This forces $X_1$ to be abelian (the centre of a group cannot have prime index), and therefore cyclic. Then by Proposition 4.1.10, $X_1$ is imprimitive, a contradiction.

Therefore $U$ is induced from a 1-dimensional module $V$ for a subgroup $H$ of index 4. This implies that $G$ has an abelian normal subgroup $B$ of exponent dividing $p^k - 1$ such that $\langle -I_4 \rangle \leq B \leq H$ and $G/B$ is isomorphic to a transitive subgroup of $S_4$. By Theorem 8.6.3 we have that $B \leq X_1$. Clearly $G/X_1 \cong A_4$. Since $S_4$ does not have $A_4$ as a quotient, we must have that $B = X_1$. So $X_1$ is abelian of exponent dividing $p^k - 1$, contradicting the irreducibility of $X_1$. ■

**8.6.5 Corollary.** *If $X_1$ is a primitive subgroup of $X$, then $X_1 \otimes GL(2,3)$ is a primitive subgroup of $M_6$.* ■

**8.6.6 Theorem.** *If $X_1$ is a primitive subgroup of $X$, then the diagonal between $X_0 \otimes SL(2,3)$ and $X_1 \otimes GL(2,3)$ is primitive.*

**Proof.** Let $G$ be the diagonal between $X_0 \otimes SL(2,3)$ and $X_1 \otimes GL(2,3)$, and suppose that $G$ is not primitive. If $X_0$ were reducible, then it would be completely

reducible and homogeneous, that is, scalar. But then $X_1$ would be imprimitive, a contradiction. Therefore $X_0$ is irreducible, and hence $G$ is irreducible. So $G$ is imprimitive. Let $U$ be the natural module for $G$.

Suppose that $U$ is induced from a 2-dimensional module for a subgroup $H$ of index 2. Then $H \trianglelefteq G$, and so $H$ contains every element of $G$ of odd order. Since $SL(2,3)$ can be generated by elements of order 3, it follows that $H \geq SL(2,3)$. If $H$ contained $X_0$, then $H$ would equal $X_0 \otimes SL(2,3)$, contradicting the reducibility of $H$. Therefore $H \not\geq X_0$, and so $G = X_0H$. It then follows that $X_1H \cap GL(2,3) = GL(2,3)$ and that $X_1 \cap H.GL(2,3)$ has index 2 in $X_1$. Every subspace of $U$ that is normalised by $I_2 \otimes GL(2,3)$ is also normalised by $I_2 \otimes SL(2,3)$. Clearly $U|_{GL(2,3)}$ (respectively $U|_{SL(2,3)}$) is the direct sum of two isomorphic absolutely irreducible modules for $GL(2,3)$ (respectively $SL(2,3)$). Therefore they normalise the same set of subspaces of $U$. Since $SL(2,3) \leq H$, it follows that $I_2 \otimes GL(2,3)$ normalises the same subspaces that $H$ normalises. Hence $H.GL(2,3)$ is reducible. But, as already mentioned, $X_1 \cap H.GL(2,3)$ has index 2 in $X_1$. By the same argument as that applied to $X_0$, this subgroup of index 2 must be irreducible. We have reached a contradiction.

Suppose that $U$ is induced from a 1-dimensional module for a subgroup $H$ of index 4. Then $G$ has an abelian normal subgroup $B$ of exponent dividing $p^k - 1$ such that $\langle -I_4 \rangle \leq B \leq H$ and $G/B$ is isomorphic to a transitive subgroup of $S_4$. By Theorem 8.6.3 we have that $B \leq X_0$. Clearly $G/X_0 \cong S_4$. Hence $B = X_0$. Therefore $X_0$ is abelian of exponent dividing $p^k - 1$, contradicting the irreducibility of $X_0$ in $GL(2,p^k)$. ∎

Now we specialise to the case $p^k = 3$. We have

$$\begin{aligned} M_6(4,3) &= M_2(2,3) \otimes M_3(2,3) \\ &= SD_{16} \otimes GL(2,3)\,. \end{aligned}$$

The primitive subgroups of $SD_{16}$ are $SD_{16}$, $Q_8$ and $C_8$. When $X_1 = X_0$, we get six groups, all of which are primitive by Theorem 8.6.4 and Corollary 8.6.5. When $X_1/X_0$ has order 2, we get five groups, all of which are primitive by Theorem 8.6.6. `ISOTEST` shows that among these eleven groups there are ten distinct isomorphism

types of Sylow 2-subgroups. The two groups whose Sylow 2-subgroups are isomorphic have derived groups of different orders. Therefore these eleven groups are pairwise non-isomorphic. None of these groups is isomorphic to a subgroup of $M_5(4,3)$ because that group is metacyclic.

So there are exactly 11 $GL(4,3)$-conjugacy classes of primitive soluble subgroups whose guardian is $M_6$.

## 8.7 The primitive subgroups of $M_7(4,p^k)$ when $p^k \equiv 3 \bmod 8$

We assume throughout this section that $p^k \equiv 3 \bmod 8$ and that $\mathbb{F}$ is the field of $p^k$ elements. Also, we denote $GL(4,\mathbb{F})$ by $L$. We established in Section 8.3 that

$$M_7(4,p^k) = C_{(p^k-1)/2} \times (GL(2,3) \operatorname{cr} S_2)\,.$$

Denote by $N$ the second direct factor in this decomposition. We must find the primitive subgroups of $N$.

**8.7.1 Proposition.** *Let $\mathbb{E}$ be a finite field, and let $A$ and $G$ be subgroups of $GL(n,\mathbb{E})$ with $A$ abelian and $G$ primitive soluble. If $G$ normalises $A$, then $G$ is contained in a primitive maximal soluble subgroup of $GL(n,\mathbb{E})$ whose unique maximal abelian normal subgroup contains $A$.*

**Proof.** Denote $GL(n,\mathbb{E})$ by $L$. Since $A$ is an abelian normal subgroup of the primitive soluble group $GA$, it follows that $A$ is homogeneous and cyclic. Consequently, $\mathbf{C}_L(A) = GL(n/m,\mathbb{K})$, for some divisor $m$ of $n$, and where $\mathbb{K}$ is a field extension of $\mathbb{E}$ of degree $m$. Then $B := \mathbf{C}_L(\mathbf{C}_L(A))$ is isomorphic to the multiplicative group of $\mathbb{K}$, and contains $A$. Since $G$ normalises $A$, it follows that $G$ normalises $B$. Let $M$ be a maximal soluble subgroup of $\mathbf{N}_L(B)$ that contains $G$. It follows from the theory in Section 2.5 that $M$ is also a maximal soluble subgroup of $L$. ∎

**8.7.2 Theorem.** *If $G$ is a primitive subgroup of $N$ that is not conjugate to a subgroup of $M_5(4,\mathbb{F})$ or $M_6(4,\mathbb{F})$, then $G$ contains* $\mathrm{Fit}(N)$.

**Proof.** (L. G. Kovács) Let $G$ be a primitive subgroup of $N$ that is not conjugate to a subgroup of $M_5$ or $M_6$. The 2-subgroups of $L$ are not primitive, and thus $G$ contains a non-trivial 3-element. The Sylow 3-subgroups of $N$ are elementary abelian of order 9. Since they are not cyclic, it follows that $O_3(G)$ is of order 1 or 3. Suppose the latter were true. Since $O_3(G)$ would not be scalar, it would follow from Proposition 8.7.1 that $G$ is conjugate to a subgroup of a JS-maximal whose unique maximal abelian normal subgroup is not scalar. The only such groups are $M_5$ and $M_6$, so we have reached a contradiction. Therefore $O_3(G) = 1$.

We have shown that $\mathrm{Fit}(G)$ is a 2-group. Since $O^+(4,2)$ (that is, $N/\mathrm{Fit}(N)$) has no non-trivial normal 2-subgroups, it follows that $\mathrm{Fit}(G) = G \cap \mathrm{Fit}(N)$. By Corollary 2.5.9, every abelian characteristic subgroup of $\mathrm{Fit}(G)$ is cyclic. If a subgroup of $D_8 \mathbin{Y} D_8$ has this property, then it is isomorphic to one of 1, $C_2$, $C_4$, $D_8$, $Q_8$, $C_4 \mathbin{Y} D_8$ and $D_8 \mathbin{Y} D_8$. Since $G$ is not a 2-group and $\mathrm{Fit}(G)$ is a 2-group, it follows that $\mathrm{Out}(\mathrm{Fit}(G))$ is not a 2-group. Therefore $\mathrm{Fit}(G)$ is isomorphic to $Q_8$, $C_4 \mathbin{Y} D_8$ or $D_8 \mathbin{Y} D_8$. Suppose the second were the case. Then $Z(G)$ would be cyclic of order 4, yet not scalar. Then by Proposition 8.7.1, $G$ would be conjugate to a subgroup of $M_5$ or $M_6$, a contradiction.

Now suppose that $\mathrm{Fit}(G) \cong Q_8$. Then $G/\mathrm{Fit}(G)$ is $C_3$ or $S_3$ (because $\mathrm{Out}(Q_8)$ is isomorphic to $S_3$). There are only two subgroups of $\mathrm{Fit}(N)$ that are isomorphic to $Q_8$, and so $G$ normalises both of them. Therefore $G$ is a subgroup of the base group $GL(2,3) \mathbin{Y} GL(2,3)$ of $N$. Denote these central factors by $X$ and $Y$. Refer to Figure 5.1 for the Burnside lattice of $GL(2,3)$. Without loss of generality we can assume that $\mathrm{Fit}(G) = \mathrm{Fit}(Y)$. Since $G/\mathrm{Fit}(G)$ has order dividing 6, it follows from Theorem 3.2.2 that $X \cap GY$ has order dividing 12. If this group were not $\langle -I_4 \rangle$, then $G$ would normalise an abelian subgroup of $X$ that was not scalar—this would imply that $G$ were conjugate to a subgroup of $M_5$ or $M_6$, a contradiction. On the other hand, if $X \cap GY$ were equal to $\langle -I_4 \rangle$, then $G$ would be a subgroup of $Y$ and so reducible, another contradiction. Hence $\mathrm{Fit}(G) \ncong Q_8$. This completes the proof. ∎

It remains only to consider the subgroups of $N$ that contain $\mathrm{Fit}(N)$. The subgroups of $O^+(4,2)$ are discussed in Appendix B. From this appendix we find

that there are 13 conjugacy classes of primitive subgroups of $N$ that contain $\mathrm{Fit}(N)$. Five of these classes contain subgroups of $M_5$ or $M_6$; the other eight do not. Thus there are eight $GL(4,p^k)$-conjugacy classes of subgroups of $N$ whose guardian is $M_7$. In particular, there are eight $GL(4,3)$-conjugacy classes of primitive soluble subgroups whose guardian is $M_7$.

## 8.8 The primitive subgroups of $M_8(4,p^k)$

We established in Section 8.4 that

$$M_8 = C_{(p^k-1)/2} \times ((D_8 \curlyvee Q_8) \leftthreetimes \mathrm{Hol}(C_5)).$$

Denote by $N$ the second direct factor in this decomposition. We wish to find the primitive subgroups of $N$. The 2-subgroups of $N$ are not primitive. Using the CAYLEY function lattice we find that there are exactly seven conjugacy classes of subgroups of $N$ which are not 2-groups. The sublattice generated by these seven classes in the Burnside lattice is shown in Figure 8.2.

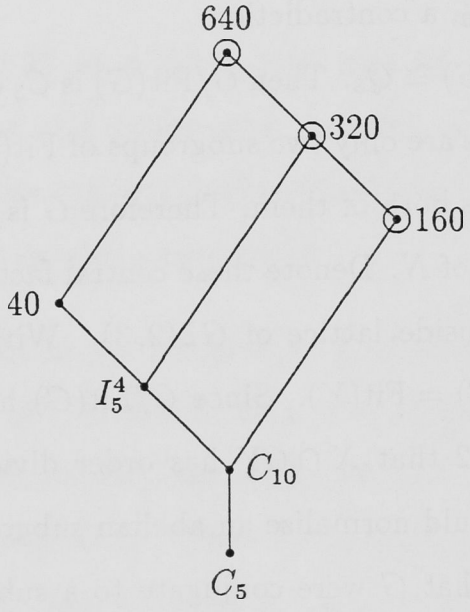



Figure 8.2: The Burnside lattice of the non-2-subgroups of $N$

Note that each subgroup of $N$ of order 40 is metacyclic. If such a group is primitive, then by Theorem 5.3.1 it is conjugate to a subgroup of $M_5(4,p^k)$. Consequently, if $G$ is a primitive subgroup of $M_8$ that is a subdirect product of a group of scalars and a subgroup of $N$ of order dividing 40, then the guardian of $G$

is $M_5$. This leaves just three subgroups of $N$ to consider. From Appendix B, the cyclic subgroups of $O^-(4,2)$ of order 5 do not fix any non-zero isotropic subspace of the natural module for $O^-(4,2)$. Therefore, by Theorem 2.5.35, each of the three remaining groups is primitive. In each of these three groups, we need to know the normal subgroups with cyclic quotients of odd order. The information in Table 8.1 shows that there are very few such normal subgroups.

| $G$ | $G'$ | $G/G'$ |
|---|---|---|
| $(D_8 \curlyvee Q_8) \leftthreetimes \mathrm{Hol}(C_5)$ | $(D_8 \curlyvee Q_8) \leftthreetimes C_5$ | $C_4$ |
| $(D_8 \curlyvee Q_8) \leftthreetimes D_{10}$ | $(D_8 \curlyvee Q_8) \leftthreetimes C_5$ | $C_2$ |
| $(D_8 \curlyvee Q_8) \leftthreetimes C_5$ | $D_8 \curlyvee Q_8$ | $C_5$ |

Table 8.1: The cyclic quotients of some primitive subgroups of $N$

By imitating the methods of Chapter 5, we could now write down the primitive subgroups of $M_8(4,p^k)$ that are not conjugate to subgroups of $M_5(4,p^k)$. It remains only to show that none of these groups is conjugate to a subgroup of $M_6(4,p^k)$ or $M_7(4,p^k)$. This follows from the fact that neither $|M_6\colon \mathrm{Fit}(M_6)|$ nor $|M_7\colon \mathrm{Fit}(M_7)|$ has 5 as a divisor.

In particular, there are exactly three $GL(4,3)$-conjugacy classes of primitive soluble subgroups whose guardian is $M_8$.

## 8.9 Summary

There are 108 $GL(4,3)$-conjugacy classes of irreducible soluble subgroups: 65 consist of imprimitive groups and 43 of primitive ones. We have picked exactly one representative from each of these classes. Tables 7.1, 8.2 and 8.3 give details about how many groups of each order there are in this set of representatives.

| order | number | order | number | order | number |
|---|---|---|---|---|---|
| 5 | 1 | 96 | 4 | 384 | 1 |
| 10 | 2 | 160 | 4 | 576 | 3 |
| 20 | 4 | 192 | 6 | 640 | 1 |
| 40 | 5 | 288 | 1 | 1152 | 3 |
| 80 | 5 | 320 | 2 | 2304 | 1 |

Table 8.2: The primitive soluble subgroups of $GL(4,3)$

| order | number | order | number | order | number |
|---|---|---|---|---|---|
| 5 | 1 | 80 | 5 | 384 | 4 |
| 10 | 2 | 96 | 9 | 512 | 1 |
| 16 | 5 | 128 | 10 | 576 | 3 |
| 20 | 4 | 160 | 4 | 640 | 1 |
| 32 | 12 | 192 | 10 | 768 | 1 |
| 40 | 5 | 256 | 6 | 1152 | 4 |
| 48 | 2 | 288 | 1 | 2304 | 3 |
| 64 | 12 | 320 | 2 | 4608 | 1 |

Table 8.3: The irreducible soluble subgroups of $GL(4,3)$

# Chapter 9

# The irreducible soluble subgroups of $GL(6,2)$

In this chapter we determine a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(6,2)$. We use the computational methods presented in Chapter 7.

## 9.1 The JS-maximals of $GL(6,p^k)$

Recall from Chapter 5 that we number the JS-maximals of $GL(2,p^k)$ as follows:

$$\begin{aligned}
M_1(2,p^k) &:= GL(1,p^k) \operatorname{wr} S_2\,, && p^k \neq 2\,,\\
M_2(2,p^k) &:= C_{p^{2k}-1} \rtimes C_2\,,\\
M_3(2,p^k) &:= (C_{p^k-1} \curlyvee Q_8) \lrcorner O^-(2,2)\,, && p^k \equiv 3 \bmod 4\,,\\
M_4(2,p^k) &:= (C_{p^k-1} \curlyvee Q_8) \lrcorner Sp(2,2)\,, && p^k \equiv 1 \bmod 4\,.
\end{aligned}$$

Recall from Chapter 6 that we number the JS-maximals of $GL(3,p^k)$ as follows:

$$\begin{aligned}
M_1(3,p^k) &:= GL(1,p^k) \operatorname{wr} S_3\,, && p^k \neq 2\,,\\
M_2(3,p^k) &:= C_{p^{3k}-1} \rtimes C_3\,,\\
M_3(3,p^k) &:= (C_{p^k-1} \curlyvee E_{27}) \lrcorner Sp(2,3)\,, && p^k \equiv 1 \bmod 3\,.
\end{aligned}$$

The JS-imprimitives of $GL(6,p^k)$ are listed below.

$$\begin{aligned}
M_1(6,p^k) &:= GL(1,p^k) \operatorname{wr} (S_2 \operatorname{wr} S_3)\,, && p^k \neq 2\,,\\
M_2(6,p^k) &:= GL(1,p^k) \operatorname{wr} (S_3 \operatorname{wr} S_2)\,, && p^k \neq 2\,,
\end{aligned}$$

$$
\begin{aligned}
M_3(6,p^k) &:= M_2(2,p^k) \text{ wr } S_3\,, \\
M_4(6,p^k) &:= M_3(2,p^k) \text{ wr } S_3\,, \quad p^k \equiv 3 \bmod 4\,, \\
M_5(6,p^k) &:= M_4(2,p^k) \text{ wr } S_3\,, \quad p^k \equiv 1 \bmod 4\,, \\
M_6(6,p^k) &:= M_2(3,p^k) \text{ wr } S_2\,, \\
M_7(6,p^k) &:= M_3(3,p^k) \text{ wr } S_2\,, \quad p^k \equiv 1 \bmod 3\,.
\end{aligned}
$$

The fact that every transitive maximal soluble subgroup of $S_6$ is conjugate to $S_2$ wr $S_3$ or $S_3$ wr $S_2$ follows from Theorems 2.1.3 and 2.1.4.

The JS-primitives of $GL(6,p^k)$ are listed below.

$$
\begin{aligned}
M_8(6,p^k) &:= C_{p^{6k}-1} \rtimes C_6\,, \\
M_9(6,p^k) &:= M_3(2,p^{3k}) \rtimes C_3\,, & p^{3k} &\equiv 3 \bmod 4\,, \\
M_{10}(6,p^k) &:= M_4(2,p^{3k}) \rtimes C_3\,, & p^{3k} &\equiv 1 \bmod 4\,, \\
M_{11}(6,p^k) &:= M_3(3,p^{2k}) \rtimes C_2\,, & p^{2k} &\equiv 1 \bmod 3\,, \\
M_{12}(6,p^k) &:= M_3(2,p^k) \otimes M_3(3,p^k)\,, & p^k &\equiv 7 \bmod 12\,, \\
M_{13}(6,p^k) &:= M_4(2,p^k) \otimes M_3(3,p^k)\,, & p^k &\equiv 1 \bmod 12\,.
\end{aligned}
$$

We have not given sufficient theory in this thesis to justify the presence and form of $M_{12}$ and $M_{13}$ in this list, and we will not do so, as neither of these groups occurs in $GL(6,2)$. The interested reader is referred to Suprunenko (1976, Theorem 20.17, p. 152).

When $p^k = 2$ there are exactly four JS-maximals, namely $M_3$, $M_6$, $M_8$ and $M_{11}$. In order to obtain their irreducible subgroups we will use the computational techniques outlined in Chapter 7.

## 9.2 A generating set for $M_{11}(6,p^k)$

Let $\mathbb{F}$ be the field of $p^k$ elements, let $x^2 + \mu x + \lambda$ be a primitive polynomial over $\mathbb{F}$, and set

$$
\bar{t} := \begin{pmatrix} 1 & 0 \\ -\mu & -1 \end{pmatrix} \text{ and } \bar{z} := \begin{pmatrix} 0 & 1 \\ -\lambda & -\mu \end{pmatrix}.
$$

Then $\bar{t}$ has order 2, $\bar{z}$ has order $p^{2k}-1$, and $\bar{z}^{\bar{t}} = \bar{z}^{p^k}$ (see Section 2.3). Let $\mathbb{E}$ be the field of order $p^{2k}$ that is the linear span of the powers of $\bar{z}$. Then $\bar{t}$ acting by conjugation induces an automorphism of $\mathbb{E}$ of order 2 which fixes $\mathbb{F}$ element-wise.

Recall that $M_{11}(6,\mathbb{F}) = M_3(3,\mathbb{E}) \rtimes C_2$. Let $\varepsilon$ be a primitive cube root of unity in $\mathbb{E}$, say $\bar{z}^{(p^{2k}-1)/3}$. From Section 6.5, we have that $M_3(3,\mathbb{E}) = \langle a, b, c, u, v, z\rangle$, where

$$a := \begin{pmatrix} I_2 & 0 & 0 \\ 0 & I_2 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad b := (I_2 - \varepsilon)^{-1} \begin{pmatrix} I_2 & \varepsilon & I_2 \\ \varepsilon & I_2 & I_2 \\ \varepsilon & \varepsilon & \varepsilon^2 \end{pmatrix},$$

$$c := (I_2 - \varepsilon)^{-1} \begin{pmatrix} I_2 & \varepsilon & \varepsilon \\ \varepsilon & I_2 & \varepsilon \\ I_2 & I_2 & \varepsilon^2 \end{pmatrix}, \quad u := \begin{pmatrix} 0 & 0 & I_2 \\ I_2 & 0 & 0 \\ 0 & I_2 & 0 \end{pmatrix},$$

$$v := \begin{pmatrix} I_2 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^2 \end{pmatrix} \text{ and } z := \begin{pmatrix} \bar{z} & 0 & 0 \\ 0 & \bar{z} & 0 \\ 0 & 0 & \bar{z} \end{pmatrix}.$$

It then follows that $M_{11}(6,\mathbb{F}) = \langle t, a, b, c, u, v, z\rangle$, where

$$t := \begin{pmatrix} \bar{t} & 0 & 0 \\ 0 & \bar{t} & 0 \\ 0 & 0 & \bar{t} \end{pmatrix}.$$

The action of $t$ on $M_3(3,\mathbb{E})$ is given in the proof of Theorem 6.5.1: if $p^k \equiv 1 \bmod 3$, then $t$ acts trivially on $a$, $b$, $c$, $u$ and $v$; otherwise we have

$$a^t = a^2, \quad b^t = c^3, \quad c^t = bc^2, \quad u^t = u \quad \text{and} \quad v^t = v^2.$$

In the case when $p^k = 2$, we have $\lambda = \mu = 1$ and so

$$\bar{t} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \bar{z} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and $\varepsilon = \bar{z}$. Furthermore, $(I_2 - \varepsilon)^{-1} = \varepsilon$. We now have a polycyclic generating sequence for $M_{11}(6,2)$.

## 9.3 The irreducible subgroups of $M_3(6,2)$

Recall that

$$\begin{aligned} M_3(6,2) &= M_2(2,2) \operatorname{wr} S_3 \\ &= GL(2,2) \operatorname{wr} S_3 . \end{aligned}$$

Therefore $M_3$ has order $2^4 3^4$. Applying lattice and then GETIRR shows that there are 19 $M_3$-conjugacy classes of irreducible subgroups of $M_3$. Let irred be a set of representatives of these classes. The orders of the groups in irred are as follows: one each of orders 9, 18, 81, 108 and 1296, two each of orders 27 and 324, three each of orders 162 and 648, and four of order 54. The two groups of order 27 are not isomorphic and so not $GL(6,2)$-conjugate. The two groups of order 324 have derived groups of different orders. The three groups of order 162 have pairwise non-isomorphic derived groups. The three groups of order 648 are pairwise non-isomorphic because they differ in the orders of their derived groups and their numbers of conjugacy classes of elements. This leaves the four groups of order 54. Denote by $E_{27}$ the extraspecial group of order 27 and exponent 3. By calculating the derived groups of the four groups of order 54, we see that one has $C_9$, one has $E_{27}$ and two have $C_3 \times C_3$. These last two have $E_{27}$ for Fitting subgroup. We know from the theory that leads to the construction of $M_{11}(6,2)$ that

$$\begin{aligned} \mathrm{N}_{GL(6,2)}(E_{27})/E_{27} &\cong M_{11}/\mathrm{Fit}(M_{11}) \\ &\cong GL(2,3)\,. \end{aligned}$$

Since $GL(2,3)$ contains a unique conjugacy class of non-central involutions, we conclude that the last two groups in irred are conjugate in $GL(6,2)$.

Thus there are exactly 18 $GL(6,2)$-conjugacy classes of irreducible soluble subgroups whose guardian is $M_3$.

## 9.4 The irreducible subgroups of $M_6(6,2)$

Recall that

$$\begin{aligned} M_6(6,2) &= M_2(3,2)\,\mathrm{wr}\,S_2 \\ &= (C_7 \rtimes C_3)\,\mathrm{wr}\,S_2\,. \end{aligned}$$

Therefore $M_6$ has order $2.3^2 7^2$. Applying lattice and then GETIRR shows that there are six $M_6$-conjugacy classes of irreducible subgroups of $M_6$. Let irred be a set of representatives of these classes. The orders of the groups in irred are as follows: one each of orders 14, 42, 98 and 882, and two of order 294. The two groups of order 294 have derived groups of different orders. So these six groups

are pairwise non-conjugate in $GL(6,2)$. Furthermore, none can be conjugate to a subgroup of $M_3$ because $M_3$ does not contain any non-trivial 7-elements.

Thus there are exactly six $GL(6,2)$-conjugacy classes of irreducible soluble subgroups whose guardian is $M_6$.

## 9.5 The irreducible subgroups of $M_8(6,2)$

Recall that $M_8(6,2) = C_{63} \rtimes C_6$. Therefore $M_8$ has order $2.3^3 7$. Applying lattice and then GETIRR shows that there are 14 $M_8$-conjugacy classes of irreducible subgroups of $M_8$. Let `irred` be a set of representatives of these classes. Five members of `irred` are $M_8$-conjugate to a group of order 54 in `irred`. This group has for its Fitting subgroup an extraspecial group of order 27 and exponent 9. This kind of Fitting subgroup is not allowed for primitive groups (see Corollary 2.5.9), and so these five groups are imprimitive. Each of the remaining nine groups in `irred` contains a cyclic group of order 21, which is primitive because it doesn't appear in our lists for $M_3$ or $M_6$. Thus these nine are primitive. The orders of these groups are as follows: one each of orders 21, 42, 189 and 378, two of order 126 and three of order 63. The two groups of order 126 have derived groups of different orders. ISOTEST shows that the three groups of order 63 are pairwise non-isomorphic.

Thus there are exactly nine $GL(6,2)$-conjugacy classes of primitive soluble subgroups whose guardian is $M_8$.

## 9.6 The irreducible subgroups of $M_{11}(6,2)$

Recall that

$$\begin{aligned} M_{11}(6,2) &= M_3(3,4) \rtimes C_2 \\ &= (E_{27} \leftthreetimes Sp(2,3)) \rtimes C_2 . \end{aligned}$$

Therefore $M_{11}$ has order $2^4 3^4$. Applying lattice and then GETIRR shows that there are 20 $M_{11}$-conjugacy classes of irreducible subgroups of $M_{11}$. Let `irred` be a set of representatives of these classes. Of the 20 groups in `irred`, 13 are contained in a group of order 324 which is clearly imprimitive because its Fitting subgroup is $C_3 \operatorname{wr} C_3$. This leaves seven groups to consider. Each of these groups contains

a subgroup that is $M_{11}$-conjugate to a particular group of order 108 in `irred`. There is only one imprimitive group of this order on our list. Comparing Sylow 2-subgroups shows that these two groups are not isomorphic. Therefore the group of order 108 in `irred` is primitive, which implies that the remaining seven groups in `irred` are also primitive. The orders of these groups are as follows: one each of orders 108, 432, 648 and 1296, and three of order 216. Comparing Sylow 2-subgroups shows that the three groups of order 216 are pairwise non-isomorphic. None of these seven groups can be conjugate to a subgroup of $M_8$ because the primitive subgroups of $M_8$ have non-trivial 7-elements.

Thus there are exactly seven $GL(6,2)$-conjugacy classes of primitive soluble subgroups whose guardian is $M_{11}$.

## 9.7 Summary

There are 40 $GL(6,2)$-conjugacy classes of irreducible soluble subgroups: 24 are imprimitive and 16 are primitive. We have picked exactly one representative from each of these classes. Table 9.1 details how many groups of each order there are in this set of representatives. Note that Harada and Yamaki (1979) also find 40 $GL(6,2)$-conjugacy classes of irreducible soluble subgroups. However, they give no indication of what the groups are or how they found them.

| order | number | order | number | order | number |
|---|---|---|---|---|---|
| 9 | 1 | 81 | 1 | 324 | 2 |
| 14 | 1 | 98 | 1 | 378 | 1 |
| 18 | 1 | 108 | 2 | 432 | 1 |
| 21 | 1 | 126 | 2 | 648 | 4 |
| 27 | 2 | 162 | 3 | 882 | 1 |
| 42 | 2 | 189 | 1 | 1296 | 2 |
| 54 | 3 | 216 | 3 | | |
| 63 | 3 | 294 | 2 | | |

Table 9.1: The irreducible soluble subgroups of $GL(6,2)$

# Chapter 10

# Conclusion

As discussed in Section 1.1, the thesis has two main objectives. One of these is to develop algorithms that take as input a positive integer $n$ and a prime $p$, and produce a list of the irreducible soluble subgroups of $GL(n,p)$. The other main objective is to execute these algorithms for those $n$ and $p$ for which $p^n < 256$, and to provide electronic access to the list of groups so obtained. The first section of this chapter summarises the results which allow construction of such a list. In the second section we discuss a CAYLEY library which provides access to the primitive soluble permutation groups of degree less than 256. In the last section we discuss work in progress on finding the conjugacy classes of irreducible soluble subgroups of $GL(8,2)$.

## 10.1 Summary of results

In this section we indicate for which $n$ and $p$ we can produce the list of irreducible soluble subgroups of $GL(n,p)$, that is, the primitive soluble subgroups of $S_{p^n}$.

$GL(1,p)$

This is a trivial case because $GL(1,p)$ is cyclic. See Remark 2.1.7.

$GL(2,p)$

There are four kinds of JS-maximals of $GL(2,p)$. The JS-imprimitive is discussed in Chapter 3. The normaliser of a Singer cycle is discussed in

Chapter 4. The other two JS-primitives are discussed in Chapter 5. Combining the results of these three chapters yields a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(2,p)$.

$GL(q,2)$, $q$ prime

By Remark 2.5.5, there are no JS-imprimitives of $GL(q,2)$. By Remark 2.5.18, the only JS-primitive is the normaliser of a Singer cycle. In Chapter 4 we give a complete and irredundant set of conjugacy class representatives of the primitive subgroups and imprimitive cyclic subgroups of this JS-primitive.

$GL(3,p)$, $p > 2$

The JS-maximals are defined in Section 6.1. When $p$ is 3 or 5 the only JS-primitive is the normaliser of a Singer cycle. The primitive subgroups of that group are determined in Chapter 4. The imprimitive soluble subgroups of $GL(3,3)$ are determined in Section 6.2. The imprimitive soluble subgroups of $GL(3,5)$ are determined in Section 6.3.

$GL(4,p)$

In Chapter 7 we define the JS-imprimitives of $GL(4,p)$, and determine the imprimitive soluble subgroups of $GL(4,3)$. The JS-primitives of $GL(4,p)$ are discussed in Chapter 8. Some work on determining their primitive subgroups is presented, in particular for the case $p \equiv 3 \bmod 8$. Specific determinations are carried out for $p$ equals 2 and 3.

$GL(5,p)$, $p > 2$

The JS-maximals are defined in Section 6.1. When $p$ is 3 the only JS-primitive is the normaliser of a Singer cycle. The primitive subgroups of that group are determined in Chapter 4. The imprimitive soluble subgroups of $GL(5,3)$ are determined in Section 6.4.

$GL(6,p)$

In Chapter 9 we define the JS-maximals of $GL(6,p)$, and determine the irreducible soluble subgroups of $GL(6,2)$.

Table 10.1 summarises the application of these results by listing the number of conjugacy classes of primitive soluble permutation groups of degree less than 256.

| Permutation degree | Group | No. of conj. classes of irred. sol. subgps | Imprim-itives | Prim-itives |
|---|---|---|---|---|
| 4 | $GL(2,2)$ | 2 | 0 | 2 |
| 8 | $GL(3,2)$ | 2 | 0 | 2 |
| 9 | $GL(2,3)$ | 7 | 2 | 5 |
| 16 | $GL(4,2)$ | 10 | 4 | 6 |
| 25 | $GL(2,5)$ | 19 | 6 | 13 |
| 27 | $GL(3,3)$ | 9 | 5 | 4 |
| 32 | $GL(5,2)$ | 2 | 0 | 2 |
| 49 | $GL(2,7)$ | 29 | 12 | 17 |
| 64 | $GL(6,2)$ | 40 | 24 | 16 |
| 81 | $GL(4,3)$ | 108 | 65 | 43 |
| 121 | $GL(2,11)$ | 42 | 12 | 30 |
| 125 | $GL(3,5)$ | 22 | 16 | 6 |
| 128 | $GL(7,2)$ | 2 | 0 | 2 |
| 169 | $GL(2,13)$ | 60 | 32 | 28 |
| 243 | $GL(5,3)$ | 16 | 8 | 8 |
| Total: | — | 370 | 186 | 184 |

Table 10.1: The primitive soluble permutation groups of degree less than 256

## 10.2 Provision of electronic access to the groups

I plan to release a CAYLEY library, IRREDSOL, in the near future that provides access to one representative of each conjugacy class of irreducible soluble subgroups of $GL(n,p)$, $p$ prime, for $n > 1$ and $p^n < 256$. At a later stage the list of groups may also be released as part of GAP.

The library comprises 15 files containing descriptions of the groups, and one other file, IRREDSOL, which contains on-line help procedures and procedures

for manipulating the groups of the library.

The group information is stored in files called GLnp (where $n$ and $p$ have specific values, for example, GL23). There are three CAYLEY objects in each such file: `fd`, `maxgens` and `gps`. `Fd` is the field of $p$ elements. `Maxgens` is a sequence: the $i$-th member is a consistent polycyclic generating sequence for the $i$-th JS-maximal of $GL(n,p)$. `Gps` is a sequence: the $i$-th member is a sequence of integers, and represents an irreducible soluble subgroup of $GL(n,p)$; we call this sequence the *compact description* of that group. The members of `gps`, when converted to the groups they represent, form a complete and irredundant set of conjugacy class representatives of the irreducible soluble subgroups of $GL(n,p)$. Each such group is stored as a subgroup of exactly one JS-maximal, namely its guardian (see Definition 2.5.39).

The following information is stored for each group $G$:

1. the (linear) degree $n$;
2. the characteristic, $p$, of the field over which $G$ is defined;
3. the position $G$ has in `gps` (see below for the way in which `gps` is ordered);
4. whether the group is imprimitive, and, if so, its minimal block size;
5. the position in `maxgens` of the polycyclic generating sequence $\mathcal{X}$ of the guardian of $G$;
6. the number of defining generators of $G$;
7. the normal forms with respect to $\mathcal{X}$ of the defining generators of $G$.

The compact descriptions are organised according to the following criteria:

1. the order of the group;
2. the number of its guardian.

We now summarise some of the procedures in IRREDSOL that can be used to manipulate the groups of the library.

GETGP is a procedure that converts a compact description into the corresponding irreducible soluble subgroup of $GL(n,p)$. GPINFO takes as input a compact description, and prints out a summary of the information stored for the corresponding group. ISIRRED takes as input a matrix group over a finite field, and returns the value true if the group is irreducible. The code for ISIRRED is listed in Appendix C. SEMIDIR takes an irreducible matrix group $G$ acting on an $n$-dimensional vector space $V$ defined over a field of prime order $p$, and returns the permutation group $H$ of degree $p^n$ that is the semidirect product of $G$ and $V$. The group $H$ acts on the set $\{1,\ldots,p^n\}$, and $G$ is isomorphic to each of the point stabilisers. From Theorem 2.1.6, $H$ is primitive, and every primitive permutation group with soluble socle arises in this way. Therefore IRREDSOL also provides access to the primitive soluble permutation groups of non-prime degrees less than 256.

### 10.2.1 Construction of the library

The following is a summary of how the files GLnp in IRREDSOL were made.

GL2p and GLq2

: I have written a program that takes as input a prime $p$ or $q$, computes **maxgens** and **gps**, and outputs the CAYLEY library file GL2p or GLq2.

GL33, GL35, GL42 and GL53

: The information in these files was obtained by using a combination of typed-in data and mechanically generated data. A program then collects and massages this information and outputs the library file.

GL43 and GL62

: **Maxgens** was typed in. The imprimitives were machine generated. For each JS-primitive, the minimal primitives were typed in, and **verband** (see Section 10.3) was used to find those subgroups containing them. A program then collects and massages this information and outputs the library file.

Part of the massaging procedure mentioned above is the conversion of the groups to their compact descriptions. The normal forms of the defining generators

of a group are computed using a simple collection procedure; the remainder of the stored information is trivial to compute.

Finally, we indicate the resources used in the construction of IRREDSOL. The timings given below are for a Sun SPARCstation 1+ with 24 megabytes of RAM. The computations have been repeated using a number of versions of CAYLEY, the most recent of which is Version 3.8-531. None of the computations used a significant amount of resources. Therefore we provide details only for the largest group, which was $M_3(4,3)$. The order of this group is 4608, the prime factorisation of which is $2^9 3^2$. Lattice can compute the lattice of $M_3(4,3)$ using a workspace of 4 megabytes, and takes about 17 minutes to do so. There are 20 598 subgroups, divided into 541 conjugacy classes. The size of the data file containing this lattice is about 3 megabytes. The rest of the algorithm, from the beginning of GETIRR to the output of the 14 compact descriptions, takes about 6 minutes. IRREDSOL is about 72 kilobytes in size. The time taken to construct the library is about 15 minutes. Note that this does not include the time taken to construct the lattices of the JS-maximals of $GL(6,2)$ and $GL(4,3)$.

### 10.2.2 Accuracy of the data

The information in the library has been checked in a number of ways. Firstly, the primitive soluble permutation groups of degree less than 81 have been determined in the literature (see Appendix A), and my count agrees with those. Secondly, each of the compact descriptions in IRREDSOL has been converted to a group by GETGP and verified to be irreducible and of the correct order. Finally, I have matched the groups of (permutation) degree less than 64 on my list with those on a list in the CAYLEY library PRMGPS due to Sims. This library contains exactly one representative of each conjugacy class of primitive subgroups of $S_m$ for every $m \leq 50$. The matching of the two lists, for degree $p^n$ say, was done in the following way.

1. Determine which of the groups on Sims' list are soluble. This can be done by using the CAYLEY boolean-valued function soluble.

2. We use SEMIDIR to convert the groups on my list to permutation groups and also to convert $GL(n,p)$ to the permutation group $AGL(n,p)$. Then each of the groups on my list is a subgroup of this one, and the socles of all these groups are the same.

3. Each of the groups on my list has the same socle, $N_1$ say. Each of the groups on Sims' list has the same socle, $N_2$ say. We look for a permutation $\pi$ that conjugates $N_2$ to $N_1$. This was done by *ad hoc* means. The typical computational step was to look in $\mathbf{C}_{S_{p^n}}(N_1 \cap N_2)$ for a permutation that conjugates an element of $N_2 \setminus (N_1 \cap N_2)$ to an element of $N_1$.

4. Conjugate the groups on Sims' list by $\pi$ so that they become subgroups of $AGL(n,p)$. Now use the CAYLEY boolean-valued function conjugate to test whether those groups are conjugate in $AGL(n,p)$ to the groups on my list.

We conjugate the socles for the following reason: $AGL(n,p)$ is a much smaller group than $S_{p^n}$, and, consequently, testing for conjugacy in the first is much faster than in the second.

## 10.3 The irreducible soluble subgroups of $GL(8,2)$

There are three JS-maximals of $GL(8,2)$; some information about them is given in Table 10.2.

| group | order | factorisation |
|---|---|---|
| $GL(2,2)$ wr $S_4$ | 31 104 | $2^7 3^5$ |
| $(C_{15} \rtimes C_4)$ wr $S_2$ | 7 200 | $2^5 3^2 5^2$ |
| $C_{255} \rtimes C_8$ | 2 040 | $2^3 3.5.17$ |

Table 10.2: The JS-maximals of $GL(8,2)$

The third of these groups has smaller order than $M_3(4,3)$, and so presents no problems different from those encountered in Chapter 7. The second of the groups is about 50% larger than $M_3(4,3)$ and so may present some computational

difficulties. However, the first of these groups is the most challenging from the point of view of finding its irreducible subgroups, so let us concentrate on that group, call it $M$. In order to deal with $M$, I propose to refine the algorithm outlined in Chapter 7. The second step of this algorithm, namely the computation of the lattice of $M$, may not be feasible. Since such a step would yield a very large number of subgroups, most of which will be reducible, it is more appropriate to use the function **verband**. This function, which permits construction of the partial lattice generated by selected subgroups, is described in detail in Cannon (1987).

Therefore, I propose the following revised algorithm for finding the irreducible subgroups of $M$.

1. If $G$ is an irreducible subgroup of $M$, then $O_2(G) = 1$ because we are in characteristic 2. Since 3 is the only other prime divisor of $|M|$, it follows that $\mathrm{Fit}(G) = O_3(G)$. Since $G$ is irreducible, $O_3(G)$ cannot have order 1 or 3. Use **verband** to build the lattice of 3-subgroups of $M$ whose order exceeds 3.

2. Clearly $G \leq \mathbf{N}_M(\mathrm{Fit}(G))$. For each 3-subgroup $F$ found in the previous step, compute its normaliser $N$ in $M$. Use `ISIRRED` to check whether $N$ is irreducible. If it is, then add $N$ to the lattice.

3. Using **verband**, add to the lattice all subgroups of $N$ which contain $F$.

4. The lattice now contains every irreducible subgroup of $M$. Apply `GETIRR` to select a set `irred` of $M$-conjugacy class representatives of the irreducible subgroups.

5. Use *ad hoc* methods to select a subset `keep` of `irred` that is a complete and irredundant set of $GL(8,2)$-conjugacy class representatives of the irreducible subgroups of $M$.

# Appendix A

# Historical notes

## A.1 Determining all permutation groups of a given degree

For this section only, we adopt the following conventions.

1. The early researchers in this area adopted the convention that the degree of a permutation group is the number of points in the set on which it acts minus the number of orbits of length 1. For example, the copy of $S_3$ in $S_4$ (a point stabiliser) was counted as a group of degree 3, not 4.

2. When we say 'all' permutation groups, we mean up to permutational isomorphism, with the definition of degree as given above.

3. We use the word 'group' to mean 'permutation group'.

4. Whenever a range of degrees is given, it is an inclusive one.

5. We make no claims on the accuracy of others' results unless explicitly stated. However, we adopt four benchmarks with which to compare all other results:

   (a) for all groups up to degree 7 we take the enumeration produced by the CAYLEY function lattice;

   (b) for the imprimitive groups up to degree 11 we take the list of Butler and McKay (1983);

(c) for the imprimitive groups of degree 12 we take the list of Royle (1987);

(d) for the primitive groups up to degree 50 we take the list of Sims, which first appeared in full in version 3.5 of CAYLEY, released in 1987.

Tables containing these figures appear at the end of the section.

The first work in this area is probably due to Ruffini (1799), who gives the possible orders of the groups of degree 5. This theme is taken up again by Cauchy (1845), who determines the possible orders of the groups of degree up to 6. Mathieu (1858) continues Cauchy's work, determining the possible orders of the groups of degrees 7 and 8. Miller (1896a) suggests that Ruffini's work is incomplete, and cites an omission in Cauchy's list for degree 6.

Serret (1850) determines all subgroups of $S_4$ and $S_5$. Miller (1896a) says that this work is correct.

Kirkman (1862-3) lists the transitive groups of degrees 3 to 10. Miller (1896a) says that this list is correct up to degree 7, has missing six groups of degree 8, another six of degree 9, and is highly inaccurate for degree 10.

Jordan (1871a), using the theory that was discussed in Chapter 2, gives a table containing the numbers of conjugacy classes of primitive maximal soluble groups of degree less than $10^6$. He claims there are five such classes of degree 81, but there are only four, as is pointed out in Chapter 8 (see page 111). This error is likely to lead to errors for larger degrees. Also, the second and third entries in the last row of this table should be swapped. In the same paper, Jordan also gives a table containing the numbers of conjugacy classes of transitive maximal soluble groups of degree up to 10 000. (This is an astounding achievement if for no other reason than the amount of counting required to prepare it. For example, if $p$ is a prime greater than 3, Jordan claims that the number of conjugacy classes of transitive maximal soluble groups of degree $2^6 3^3 p$ is 8306.) Again, the error in the first table is likely to lead to errors in this one too. Jordan (1872) counts all the primitive groups of degrees 4 to 17. His count matches that of Sims except that Jordan has one less for degrees 9, 12 and 15, eight less for degree 16 and two less for degree 17. These errors are pointed out by Miller (1894b, 1895c, 1897a,

1897b and 1900a). Jordan (1874) states that every transitive group of degree 19 is either alternating, symmetric or affine. This agrees with Sims' list.

Veronese (1883) determines all groups of degree up to 6. Miller (1935) cites several errors for degree 6.

Askwith (1890a) and Cayley (1891) determine the groups of degree 6 and get the same answers. Their count of the intransitive ones is correct but they undercount the transitive groups by three, as Cole (1893a) points out. As Kirkman (1862-3) had already (successfully, according to Miller) determined the transitives, degree 6 was then complete.

Askwith (1890a) and Cayley (1891) also arrive at the same determination of the groups of degree 7. They undercount both the transitives and intransitives by one, as Cole (1893a) points out. With Kirkman's transitives and Cole's additional intransitive, degree 7 was then complete.

Askwith (1890b) and Cayley (1891) determine the groups of degree 8, but this time they differ; Cayley points out a number of errors in Askwith's list. Cole (1893a) exhibits 40 groups missing from Cayley's list, 20 transitive and 20 intransitive. Askwith's list is similarly inaccurate. However, Miller (1894a) points out that two of the 'new' groups of degree 8 given by Cole are equal, and also produces an imprimitive group of degree 8 that he claims is neither on Cayley's list nor Cole's. Miller (1894b) produces a second group of degree 8 (a primitive one) that he claims both Cayley and Cole missed. He says that this group can be found in both Kirkman (1862-3) and Jordan (1871b). No further corrections have been made to the lists for degree 8; their number stands at 200, with 50 being transitive, and 7 primitive.

Askwith (1893) determines the transitive groups of degree 9. Cole (1893b and 1893c) determines the groups of degree 9, and finds 12 more transitive ones than Askwith. Cole's numbers for the transitive groups agree with those of Butler and McKay (1983) and Sims (1970). Miller (1894b) gives two intransitive groups that are not on Cole's list. No further corrections have been made to the lists for degree 9; their number stands at 258, with 34 being transitive, and 11 primitive.

Cole (1895) lists the transitive groups of degree 10. Miller (1895a) shows that Cole's list of imprimitive groups has six repetitions. With these corrections, Cole's numbers for the transitive groups agree with those of Butler and McKay (1983) and Sims (1970). Miller (1895b) gives a list of the intransitive groups of degree 10; it contains 994 such groups. Miller (1900b) gives what he considers a formal derivation of the primitive groups of degree 10.

Cole (1895) determines the transitive groups of degree 11. His list agrees with that of Sims (1970). Miller and Ling (1901) determine the intransitive groups of degree 11; they find 1492 such groups.

Miller (1895c and 1896b) determines the transitive groups of degree 12. His count for the primitives matches that of Sims (1970), but for the imprimitives it differs from that of Royle (1987) in several places.

Miller (1897a, 1897b, 1898a, 1898b and 1900a) determines the primitive groups of degrees 13 to 17. His enumerations agree with those of Sims (1970). In (1898a) he also determines the imprimitive groups of degree 14, obtaining 59.

Miller (1898b) correctly gives a table of the numbers of soluble primitive groups of degree up to 24.

Burnside (1897) determines all primitive groups of degrees 3 to 8. His work is correct, except that he obtains two non-existent primitive groups of degree 8, their construction having been left as an exercise. This error also occurs in the second edition (1911) of his book, despite Miller (1899) having pointed it out.

Martin (1901) and Kuhn (1904) determine the imprimitive groups of degree 15; they both find 70.

Martin (1901) determines the primitive groups of degree 18; her list agrees with that of Sims.

Bennett (1912) determines the primitive groups of degree 20; her list agrees with that of Sims.

There does not seem to be any more literature on this topic until Sims (1970) lists all primitive groups of degrees up to 20. He says that he took the list from the literature and verified it partly by hand and partly by machine. He later extended this list to degree 50. Although the full list has never been published, it

was made available in version 3.5 of CAYLEY, released in 1987, as the CAYLEY library PRMGPS.

In Harada and Yamaki (1979), there is an undated reference to a master's thesis by Mizutani; the title of the thesis is "The classification of primitive permutation groups of degree less than 49". No material from this thesis seems to have been published.

Pogorelov (1980 and 1982) lists, up to isomorphism, all primitive groups with insoluble socle for degrees 21 to 64. This work was done by hand using M. Hall's classification of simple groups of order less than $10^6$ and various theorems on simple groups and primitive groups. Unfortunately he does not tabulate his results and so it is difficult to compare his list with that of Sims.

Butler and McKay (1983) determine, with the help of CAYLEY, all imprimitive groups up to degree 11. Royle (1987) makes considerable use of CAYLEY to determine all imprimitive groups of degree 12. In version 3.6 of CAYLEY, released in 1987, Royle provides a library, TRNGPS, containing all transitive groups of degree up to 12. For the primitive groups he relies on Sims' list, but for the imprimitive groups he uses the methods he developed for degree 12. He says that his list matches that of Butler and McKay.

Tang and Wang (1988) determine by hand the primitive groups of degrees 21 to 30. Their count agrees with that of Sims.

Il'in and Takmakov (1986) determine the simple primitive groups of degree up to 1000. Dixon and Mortimer (1988) list the primitive groups of degree less than 1000 that have insoluble socle. Their calculations are done by hand, but depend on the classification of finite simple groups, and on the detailed information in the Atlas (Conway et al. (1985)). They point out some errors in the list of Il'in and Takmakov.

The following two tables give the numbers of permutation groups of various kinds from degree 1 to 50. The figures up to degree 7 are those produced by lattice, the figures for degrees 8 to 12 are those of Royle (1987) from TRNGPS, and the figures for degrees 13 to 50 are those of Sims from PRMGPS.

| Degree | Total | Primitive | Imprimitive | Intransitive |
|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 0 | 0 |
| 3 | 2 | 2 | 0 | 0 |
| 4 | 7 | 2 | 3 | 2 |
| 5 | 8 | 5 | 0 | 3 |
| 6 | 37 | 4 | 12 | 21 |
| 7 | 40 | 7 | 0 | 33 |
| 8 | | 7 | 43 | |
| 9 | | 11 | 23 | |
| 10 | | 9 | 36 | |
| 11 | | 8 | 0 | |
| 12 | | 6 | 295 | |

Table A.1: The number of permutation groups of degrees 1 to 12

## A.2 Determining irreducible subgroups of linear groups over finite fields

There have been numerous papers devoted to determining certain subgroups of certain linear groups (especially the projective special linear groups), but we mention only those that might help us understand the irreducible subgroups of general linear groups over finite fields, symplectic groups over finite prime fields, and orthogonal groups over the field of 2 elements. Throughout this section $p$ is a prime and $k$ is a positive integer.

As was mentioned in the previous section, Jordan (1871a) essentially gives a table containing the numbers of conjugacy classes of maximal irreducible soluble subgroups of $GL(n,p)$ for $p^n < 10^6$. He claims there are five such classes in $GL(4,3)$, but there are only four, as was pointed out in Chapter 8 (see page 111). This error is likely to lead to errors for larger degrees. Also, the second and third entries in the last row of this table should be swapped.

Dickson (1901, Chapter 12, pp. 260-287) determines all subgroups of $PSp(2,p^k)$

| Degree | Primitive | Degree | Primitive | Degree | Primitive |
|---|---|---|---|---|---|
| 13 | 9 | 26 | 7 | 39 | 2 |
| 14 | 4 | 27 | 15 | 40 | 8 |
| 15 | 6 | 28 | 14 | 41 | 10 |
| 16 | 22 | 29 | 8 | 42 | 4 |
| 17 | 10 | 30 | 4 | 43 | 10 |
| 18 | 4 | 31 | 12 | 44 | 4 |
| 19 | 8 | 32 | 7 | 45 | 9 |
| 20 | 4 | 33 | 4 | 46 | 2 |
| 21 | 9 | 34 | 2 | 47 | 6 |
| 22 | 4 | 35 | 6 | 48 | 4 |
| 23 | 7 | 36 | 22 | 49 | 40 |
| 24 | 5 | 37 | 11 | 50 | 9 |
| 25 | 28 | 38 | 4 | | |

Table A.2: The number of primitive permutation groups of degrees 13 to 50

(for a determination in modern terminology, see Huppert (1967, Chapter 2, Section 8, pp. 191-214)) and in (1904) he determines all subgroups of $PSp(4,3)$.

Mitchell (1914) determines the maximal subgroups of $PSp(4,p^k)$ for odd $p$.

Liskovec (1973) classifies the maximal irreducible $\{p,q\}$-subgroups of $GL(r^2,p)$, where $q$ and $r$ are primes and $q$ is odd.

Conlon (1977) determines the non-abelian $q$-subgroups ($q$ prime) of $GL(q,p^k)$ and the non-abelian 2-subgroups of $Sp(2,p^k)$.

Harada and Yamaki (1979) count the irreducible subgroups of $GL(n,2)$ for $n \leq 6$. They do not describe their methods, and the only groups they list are the insoluble ones for $n = 6$. Their count for the soluble groups of these degrees is correct.

Kondrat'ev (1985, 1986a, 1986b and 1987) determines the irreducible subgroups of $GL(7,2)$, the insoluble irreducible subgroups of $GL(8,2)$ and $GL(9,2)$, and the insoluble primitive subgroups of $GL(10,2)$.

# Appendix B

# The subgroups of $O^+(4,2)$ and $O^-(4,2)$

This appendix contains some facts about the subgroup structure of $O^+(4,2)$ and $O^-(4,2)$. These facts are used in Chapter 8 in our analysis of the primitive soluble subgroups of $GL(4,p^k)$.

Recall that we are using the notations $Sp(4,2)$, $O^+(4,2)$ and $O^-(4,2)$ to refer to specific subgroups of $GL(4,2)$. See Notation 2.4.18.

## B.1 The subgroups of $O^+(4,2)$

First we describe how to find a generating set for $O^+(4,2)$. CAYLEY has a built-in function which sets up a symplectic group of dimension 4 over the field of 2 elements. However, it is not the symplectic group we want, so first we conjugate the given generating set by a suitable matrix (which is easy to find) so that we have $Sp(4,2)$. This group has order just 720 and so it is easy to search through all of its elements and locate those which satisfy the requirements to be a member of $O^+(4,2)$. Note that $O^+(4,2)$ is isomorphic to $S_3 \operatorname{wr} S_2$ and so has order 72.

We think of $O^+(4,2)$ as the outer automorphism group of $E := D_8 \curlyvee D_8$. Then the natural module for $O^+(4,2)$ is $E/A$, where $A$ is the centre of $E$. In this context, we then say that the *preimage* of a subspace $B/A$ of $E/A$ is the subgroup $B$ of $E$. Denote $O^+(4,2)$ by $L$. It turns out that two subspaces of $E/A$

are in the same $L$-orbit if and only if they have the same preimage. Table B.1 lists all preimages together with the normaliser of a corresponding subspace. In this table, if there is more than one conjugacy class of subgroups (abstractly) isomorphic to $\mathrm{N}_L(B/A)$, then we list the number of that class (in CAYLEY's enumeration via lattice) in square brackets.

| preimage $B$ | $L$-orbit length | $\mathrm{N}_L(B/A)$ |
|---|---|---|
| $C_2$ | 1 | $O^+(4,2)$ |
| $C_4$ | 6 | $D_{12}$ [19] |
| $C_2 \times C_2$ | 9 | $D_8$ |
| $C_4 \times C_2$ | 9 | $D_8$ |
| $D_8$ | 18 | $C_2 \times C_2$ [9] |
| $Q_8$ | 2 | $S_3 \times S_3$ [24] |
| $C_2 \times C_2 \times C_2$ | 6 | $D_{12}$ [18] |
| $D_8 \times C_2$ | 9 | $D_8$ |
| $D_8 \curlyvee C_4$ | 6 | $D_{12}$ [19] |
| $D_8 \curlyvee D_8$ | 1 | $O^+(4,2)$ |

Table B.1: Subspace normalisers in $O^+(4,2)$

Let $\mathcal{S}$ be a complete and irredundant set of $L$-conjugacy class representatives of the subgroups of $L$. The cardinality of $\mathcal{S}$ is 26. We need to determine the members of $\mathcal{S}$ which normalise a maximal isotropic subspace (see Theorem 8.3.2). The maximal isotropic subspaces are those whose preimages are abelian of order 8. The normaliser of such a subspace is $D_8$ or $D_{12}$ [18]. There are 13 groups in $\mathcal{S}$ which lie in one of these groups. These correspond to the subgroups of $N$ that are imprimitive, where $N := E \wr L$. Therefore the other 13 groups in $\mathcal{S}$ correspond to the subgroups of $N$ that are primitive. Five of these are subgroups of $D_{12}$ [19], and the other eight are supergroups of $C_3 \times C_3$.

Consider the five subgroups of $D_{12}$ [19]. These normalise a 1-dimensional subspace whose preimage is $C_4$. Therefore the corresponding subgroups of $N$ normalise a $C_4$, which is not scalar. By Proposition 8.7.1, these groups must be conjugate to subgroups of $M_5(4,p^k)$ or $M_6(4,p^k)$.

Consider the eight supergroups of $C_3 \times C_3$. The corresponding subgroups of $N$ have 9 as a divisor of the index of their Fitting subgroup. The Fitting subgroup of $M_5(4, p^k)$ has index dividing 4, and the Fitting subgroup of $M_6(4, p^k)$ has index dividing 12. Therefore these eight subgroups of $N$ are not conjugate to subgroups of $M_5$ or $M_6$.

Thus there are eight $GL(4, p^k)$-conjugacy classes of subgroups of $N$ whose guardian is $M_7$.

## B.2 The subgroups of $O^-(4, 2)$

We find a generating set for $O^-(4, 2)$ in the same way as we did for $O^+(4, 2)$. The following three matrices generate $O^-(4, 2)$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Note that $O^-(4, 2)$ is isomorphic to $S_5$ and so has order 120.

We think of $O^-(4, 2)$ as the outer automorphism group of $E := D_8 \circ Q_8$. Then the natural module for $O^-(4, 2)$ is $E/A$, where $A$ is the centre of $E$. Denote $O^-(4, 2)$ by $L$. It turns out that two subspaces of $E/A$ are in the same $L$-orbit if and only if they have the same preimage. Table B.2 lists all preimages together with the normaliser of a corresponding subspace.

Since $L$ is not soluble, we must determine its completely reducible maximal soluble subgroups that fix no non-zero isotropic subspaces (see Theorem 2.5.32). Let $\mathcal{S}$ be a complete and irredundant set of $L$-conjugacy class representatives of the subgroups of $L$. The cardinality of $\mathcal{S}$ is 19. We find that there are just five members of $\mathcal{S}$ which fix no non-zero isotropic subspace: they are $C_5$, $D_{10}$, $\mathrm{Hol}(C_5)$, $A_5$ and $O^-(4, 2)$. One of these is maximal soluble, namely $\mathrm{Hol}(C_5)$. This justifies the existence of $M_8(4, p^k)$.

| preimage $B$ | $L$-orbit length | $\mathbf{N}_L(B/A)$ |
|---|---|---|
| $C_2$ | 1 | $O^-(4,2)$ |
| $C_4$ | 10 | $D_{12}$ |
| $C_2 \times C_2$ | 5 | $S_4$ |
| $C_4 \times C_2$ | 15 | $D_8$ |
| $D_8$ | 10 | $D_{12}$ |
| $Q_8$ | 10 | $D_{12}$ |
| $Q_8 \times C_2$ | 5 | $S_4$ |
| $D_8 \curlyvee C_4$ | 10 | $D_{12}$ |
| $D_8 \curlyvee Q_8$ | 1 | $O^-(4,2)$ |

Table B.2: Subspace normalisers in $O^-(4,2)$

# Appendix C

# Program listings

The code for ISOTEST is about 2800 lines long. Instead of listing it all, we give an example of a procedure called by ISOTEST, namely the procedure which identifies the groups of order $p^2q$, where $p$ and $q$ are distinct primes. The other procedures are of a similar nature. Note that Hölder (1893) was the first to correctly determine the groups of order $p^2q$. These groups are also listed by Neubüser (1967).

```
"This is a procedure for identifying groups of order p^2q, where p
and q are distinct primes. I divide the non-abelian groups into
families. Not all families are defined for all values of p and q.
If a family consists of a single group, then its name is
of the form p^2q#xy, where x is the generator number, and y is a
letter. If the family consists of more than one group, then I
append the character * so that the name is p^2q#xy*.
The families, with their existence criteria, are as follows:
#2a   .....  p|(q-1)
#2b   .....  p^2|(q-1)
#2c   .....  p|(q-1)
#2d   .....  q|(p-1)
#2e   .....  q|(p-1)
#2f*  .....  q <> 2, q|(p-1)  ..... family of (q-1)/2 groups
#2g   .....  q <> 2, q|(p+1)
#3a   .....  q|(p-1)"

"Take the group GP of order P^2*Q, where P and Q are distinct
primes, and return the family number FAMNMR and, if possible, the
name NAME, of GP."

procedure isop2q( gp, p, q; famnmr, name );
    famnmr = '';
    name = '';
    if cyclic( gp ) then
```

```
    name = 'C(p^2q)';
    return;
end;
if abelian( gp ) then
    name = 'Ab(pq,p)';
    return;
end;

if q mod p eq 1 then
    der = derived group( gp );
    if not cyclic( der ) then
        famnmr = 'p^2q # 2g';
        name = 'A(4)';
        return;
    end;
    if not cyclic( gp/der ) then
        famnmr = 'p^2q # 2c';
        if p eq 2 then
            name = 'D(4q)';
        else
            name = 'pq#2a x C(p)';
        end;
        return;
    end;
    if order( centraliser( gp, der ) ) eq q then
        famnmr = 'p^2q # 2b';
        if ( p eq 2 ) and ( q eq 5 ) then
            name = 'Hol C(5)';
        end;
    else
        famnmr = 'p^2q # 2a';
        if p eq 2 then
            name = 'I(q,4)';
        end;
    end;
    return;
end;

if ( q ne 2 ) and ( p mod q eq ( q - 1 ) ) then
    famnmr = 'p^2q # 2g';
    return;
end;

der = derived group( gp );
if cyclic( der ) then
    if cyclic( centraliser( gp, der ) ) then
        famnmr = 'p^2q # 2d';
        if q eq 2 then
            name = 'D(2p^2)';
        end;
    else
        famnmr = 'p^2q # 2e';
```

```
            if q eq 2 then
                if p eq 3 then
                    name = 'S(3) x C(3)';
                else
                    name = 'D(2p) x C(p)';
                end;
            else
                name = 'qp#2a x C(p)';
            end;
        end;
    else
        if length( minimal normals( gp ) ) eq 2 then

        "This is a family of (Q-1)/2 groups that have identical
        subgroup lattices. Consequently, we do not attempt to
        distinguish them."

            famnmr = 'p^2q # 2f*';
        else
            famnmr = 'p^2q # 3a';
        end;
    end;
end; "isop2q"
```

Now we list the code for ISIRRED, the procedure used to test whether a matrix group is irreducible or not.

```
"Take the matrix group GP defined over a finite field, determine
whether it is irreducible, and return the (boolean) answer as
IRRED. The test of irreducibility is done by computing the orbits
of the 1-dimensional vector subspaces under the action of GP, and
then looking at the dimensions of the submodules generated by
these orbits."

procedure isirred( gp; irred );
    n = size( gp );
    matorb = matrix orbits( gp, true );
    len = length( matorb );
    irred = true;
    i = 0;
    while ( irred ) and ( i lt len ) do
        i = i + 1;
        subgens = matrix orbit( gp, matorb[ i ], true );
        submod = < subgens >;
        irred = dimension( submod ) eq n;
    end;
end; "isirred"
```

Finally, we list the code for GETIRR. We mention that the *Burnside matrix* of a partial lattice of subgroups of a group is a matrix whose $(i, j)$-th entry is the

number of groups in the $i$-th conjugacy class of subgroups that contain or are contained in the representative of the $j$-th conjugacy class.

```
"Take a finitely presented group GP, its lattice LAT, its Burnside
matrix BURN, a sequence BIGRED of subgroups of GP, a matrix group
MGP, and a faithful representation PHI from GP to MGP such that
the image of each member of BIGRED is reducible. Return the
sequence IRRED of index positions of the members of LAT whose
images are irreducible."

procedure getirr( gp, lat, burn, bigred, mgp, phi; irred );
    n = size( mgp );
    irred = empty;
    len = length( lat );

    "Attach to each member of LAT a boolean value and store these
    in CHECK. If CHECK[ i ] is true, then we don't know whether
    LAT[ i ] is irreducible or not. If CHECK[ i ] is false, then
    we do know which it is."

    check = conseq( true, len );

    "Subgroups of reducible groups are reducible."

    for i = 1 to length( bigred ) do
        bignum = lattice class( lat, bigred[ i ] );
        for j = 1 to bignum do
            if check[ j ] then
                check[ j ] = fetch( burn, j, bignum ) eq 0;
            end;
        end;
    end;

    for i = 1 to len do
        if not check[ i ] then
            loop;
        end;
        isirred( phi( lat[ i ] ); irr );
        if irr then
            irred = append( irred, i );

            "Supergroups of irreducible groups are irreducible."

            for j = i + 1 to len do
                if check[ j ] then
                    check[ j ] = fetch( burn, i, j ) eq 0;
                    if not check[ j ] then
                        irred = append( irred, j );
                    end;
                end;
            end;
        end;
```

```
    end;

end; "getirr"
```

# Bibliography


E. H. Askwith (1890a), "On possible groups of substitutions that can be formed with three, four, five, six and seven letters respectively", *Quart. J. Pure Appl. Math.* **24**, 111-167.

E. H. Askwith (1890b), "On groups of substitutions that can be formed with eight letters", *Quart. J. Pure Appl. Math.* **24**, 263-331.

E. H. Askwith (1893), "On groups of substitutions that can be formed with nine letters", *Quart. J. Pure Appl. Math.* **26**, 79-128.

David Baldwin (1987), "The groups of order $3^n$, for $n \leq 6$", BSc thesis, Australian National University.

Elizabeth R. Bennett (1912), "Primitive groups with a determination of the primitive groups of degree 20", *Amer. J. Math.* **34**, 1-20.

Beverley Bolt, T. G. Room and G. E. Wall (1961-62), "On the Clifford collineation, transform and similarity groups. I and II", *J. Aust. Math. Soc.* **2**, 60-96.

W. Burnside (1897), *Theory of Groups of Finite Order*, 1st edn, Cambridge University Press.

W. Burnside (1911), *Theory of Groups of Finite Order*, 2nd edn, Cambridge University Press. Reprinted by Dover, New York, 1955.

Gregory Butler and John McKay (1983), "The transitive groups of degree up to eleven", *Comm. Algebra* **11**, 863-911.

John J. Cannon (1984), "An introduction to the group theory language, Cayley", in *Computational Group Theory*, ed. Michael D. Atkinson, Academic Press, London, pp. 145-183.

John Cannon (1987), "The subgroup lattice module", in *The CAYLEY Bulletin*, no. 3, ed. John Cannon, Department of Pure Mathematics, University of Sydney, pp. 42-69.

A. L. Cauchy (1845), *C. R. Acad. Sci.* **21**, 1363-1369.

A. Cayley (1891), "On the substitution groups for two, three, four, five, six, seven, and eight letters", *Quart. J. Pure Appl. Math.* **25**, 71-88, 137-155.

F. N. Cole (1893a), "Note on the substitution groups of six, seven, and eight letters", *Bull. New York Math. Soc.* **2**, 184-190.

F. N. Cole (1893b), "The transitive substitution-groups of nine letters", *Bull. New York Math. Soc.* **2**, 250-258.

F. N. Cole (1893c), "List of the substitution groups of nine letters", *Quart. J. Pure Appl. Math.* **26**, 372-388.

F. N. Cole (1895), "List of the transitive substitution groups of ten and of eleven letters", *Quart. J. Pure Appl. Math.* **27**, 39-50.

S. B. Conlon (1977), "Nonabelian subgroups of prime-power order of classical groups of the same prime degree", in *Group Theory*, eds R. A. Bryce, J. Cossey and M. F. Newman, Lecture Notes in Mathematics 573, Springer-Verlag, Berlin, Heidelberg, pp. 17-50.

J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson (1985), *Atlas of Finite Groups*, Clarendon Press, Oxford.

Leonard Eugene Dickson (1901), *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig. Reprinted by Dover, New York, 1958.

Leonard Eugene Dickson (1904), "Determination of all the subgroups of the known simple group of order 25920", *Trans. Amer. Math. Soc.* **5**, 126-166.

J. Dieudonné (1961), "Notes sur les travaux de C. Jordan relatifs à la théorie des groupes finis", in *Oeuvres de Camille Jordan*, tome 1, Gauthier-Villars, Paris, pp. XVII-XLII.

John D. Dixon (1971), *The Structure of Linear Groups*, Van Nostrand Reinhold, London.

John D. Dixon and Brian Mortimer (1988), "The primitive permutation groups of degree less than 1000", *Math. Proc. Camb. Philos. Soc.* **103**, 213-238.

Koichiro Harada and Hiroyoshi Yamaki (1979), "The irreducible subgroups of $GL_n(2)$ with $n \leq 6$", *C. R. Math. Rep. Acad. Sci. Canada* **1**, 75-78.

George Havas and L. G. Kovács (1984), "Distinguishing eleven crossing knots", in *Computational Group Theory*, ed. Michael D. Atkinson, Academic Press, London, pp. 367-373.

Otto Hölder (1893), "Die Gruppen der Ordnungen $p^3$, $pq^2$, $pqr$, $p^4$", *Math. Ann.* **43**, 301-412.

B. Huppert (1967), *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg.

B. Huppert and N. Blackburn (1982), *Finite Groups II*, Springer-Verlag, Berlin, Heidelberg.

V. I. Il'in and A. S. Takmakov (1986), "Primitive simple permutation groups of small degrees", *Algebra and Logic* **25**, 167-171.

I. M. Isaacs (1975), "Character degrees and derived length of a solvable group", *Canad. J. Math.* **27**, 146-151.

C. Jordan (1867), "Mémoire sur la résolution algébrique des équations", *C. R. Acad. Sci.* **64**, 269-272, 586-590, 1179-1183.

C. Jordan (1868), "Sur la résolution algébrique des équations primitives de degré $p^2$ ($p$ étant premier impair)", *J. de Math.* (2) **13**, 111-135.

C. Jordan (1871a), "Sur la résolution des équations les unes par les autres", *C. R. Acad. Sci.* **72**, 283-290.

C. Jordan (1871b), "Sur la classification des groupes primitifs", *C. R. Acad. Sci.* **73**, 853-857.

C. Jordan (1872), "Sur l'énumération des groupes primitifs pour les dix-sept premiers degrés", *C. R. Acad. Sci.* **75**, 1754-1757.

C. Jordan (1874), "Sur deux points de la théorie des substitutions", *C. R. Acad. Sci.* **79**, 1149-1151.

C. Jordan (1917), "Mémoire sur les groupes résolubles", *J. de Math.* (7) **3**, 263-374.

H. Jürgensen (1970), "Calculation with the elements of a finite group given by generators and defining relations", in *Computational Problems in Abstract Algebra*, ed. John Leech, Pergamon Press, Oxford, pp. 47-57.

T. P. Kirkman (1862-3), "The complete theory of groups, being the solution of the mathematical prize question of the French Academy for 1860", *Proc. Manchester Lit. Philos. Soc.* **3**, 133-152, 161-162. Erratum: *ibid.* **4** (1865), 171-172.

A. S. Kondrat'ev (1985), "Irreducible subgroups of the group $GL(7,2)$", *Mat. Zametki* **37**, 317-321.

A. S. Kondrat'ev (1986a), "Irreducible subgroups of the group $GL(9,2)$", *Mat. Zametki* **39**, 320-329.

A. S. Kondrat'ev (1986b), "Linear groups of small degree over a field of order 2", (Russian), *Algebra i Logika* **25**, 544-565.

A. S. Kondrat'ev (1987), "The irreducible subgroups of the group $GL_8(2)$", *Comm. Algebra* **15**, 1039-1093.

H. W. Kuhn (1904), "On imprimitive substitution groups", *Amer. J. Math.* **26**, 45-102.

Martin W. Liebeck, Cheryl E. Praeger and Jan Saxl (1988), "On the O'Nan-Scott theorem for finite primitive permutation groups", *J. Austral. Math. Soc. (Series A)***44**, 389-396.

S. G. Liskovec (1973), "Maximal biprimary permutation groups", (Russian), *VescīAkad. Navuk BSSR Ser. Fīz.-Mat. Navuk* **1973**, no. 6, 13-17.

E. N. Martin (1901), "On the imprimitive substitution groups of degree fifteen and the primitive substitution groups of degree eighteen", *Amer. J. Math.* **23**, 259-286.

É. Mathieu (1858), *C. R. Acad. Sci.* **46**, 1048, 1208.

G. A. Miller (1894a), "Note on substitution groups of eight letters", *Bull. New York Math. Soc.* **3**, 168-169.

G. A. Miller (1894b), "Note on the substitution groups of eight and nine letters", *Bull. New York Math. Soc.* **3**, 242-245.

G. A. Miller (1895a), "On the non-primitive substitution-groups of degree ten", *Bull. Amer. Math. Soc.* (2) **1**, 67-72.

G. A. Miller (1895b), "Intransitive substitution groups of ten letters", *Quart. J. Pure Appl. Math.* **27**, 99-118.

G. A. Miller (1895c), "Note on the transitive substitution groups of degree twelve", *Bull. Amer. Math. Soc.* (2) **1**, 255-258.

G. A. Miller (1896a), "On the lists of all the substitution groups that can be formed with a given number of elements", *Bull. Amer. Math. Soc.* (2) **2**, 138-145.

G. A. Miller (1896b), "List of transitive substitution groups of degree twelve", *Quart. J. Pure Appl. Math.* **28**, 193-231. Erratum: *Quart. J. Pure Appl. Math.* **29** (1898), 249.

G. A. Miller (1897a), "On the primitive substitution groups of degree fifteen", *Proc. London Math. Soc.* (1) **28**, 533-544.

G. A. Miller (1897b), "Sur l'énumération des groupes primitifs dont le degré est inférieur à 17", *C. R. Acad. Sci.* **124**, 1505-1508.

G. A. Miller (1898a), "On the transitive substitution groups of degrees thirteen and fourteen", *Quart. J. Pure Appl. Math.* **29**, 224-249.

G. A. Miller (1898b), "On the primitive substitution groups of degree sixteen", *Amer. J. Math.* **20**, 229-241.

G. A. Miller (1899), "Note on Burnside's Theory of Groups", *Bull. Amer. Math. Soc.* (2) **5**, 249-251.

G. A. Miller (1900a), "On the transitive substitution groups of degree seventeen", *Quart. J. Pure Appl. Math.* **31**, 49-57.

G. A. Miller (1900b), "On the primitive substitution groups of degree ten", *Quart. J. Pure Appl. Math.* **31**, 228-233.

G. A. Miller and G. H. Ling (1901), "List of the intransitive substitution groups of degree eleven", *Quart. J. Pure Appl. Math.* **32**, 342-368.

G. A. Miller (1935), "Historical note on the determination of all the permutation groups of low degrees", in *The Collected Works of George Abram Miller*, vol. 1, University of Illinois, Urbana, Illinois, pp. 1-9.

Howard H. Mitchell (1914), "The subgroups of the quaternary abelian linear group", *Trans. Amer. Math. Soc.* **15**, 379-396.

Joachim Neubüser (1967), "Die Untergruppenverbände der Gruppen der Ordnungen $\leq 100$ mit Ausnahme der Ordnungen 64 und 96", Habilitationsschrift, Kiel.

M. F. Newman (1976), "Calculating presentations for certain kinds of quotient groups", *SYMSAC '76*, Association for Computing Machinery, New York, pp. 2-8.

M. F. Newman and E. A. O'Brien (1989), "A CAYLEY library for the groups of order dividing 128", in *Group Theory*, eds K. N. Cheng and Y. K. Leong, Walter de Gruyter, Berlin, New York, pp. 437-442.

W. Nickel, A. Niemeyer and M. Schönert (1988), GAP *Getting started and reference manual*, Lehrstuhl D für Mathematik, RWTH Aachen.

B. A. Pogorelov (1980), "Primitive permutation groups of low degree", *Algebra and Logic* **19**, 230-254, 278-296.

B. A. Pogorelov (1982), "Primitive permutation groups of degree $n \in \overline{\{51, 64\}}$", in *Eighth All-Union Symposium on Group Theory*, Abstracts of Reports, Institute of Mathematics, Academy of Sciences of the UkrSSR, Kiev, p. 98.

Robert Remak (1930), "Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte", *J. Reine Angew. Math.* **163**, 1-44.

Derek J. S. Robinson (1982), *A Course in the Theory of Groups*, Springer-Verlag, New York.

Gordon F. Royle (1987), "The transitive groups of degree twelve", *J. Symbolic Comput.* **4**, 255-268.

P. Ruffini (1799), "Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto", 2 vols, Bologna.

J.-A. Serret (1850), "Mémoire sur les fonctions de quatre, cinq et six lettres", *J. Math. Pures Appl.* (1) **15**, 45-70.

Charles C. Sims (1970), "Computational methods in the study of permutation groups", in *Computational Problems in Abstract Algebra*, ed. John Leech, Pergamon Press, Oxford, pp. 169-183.

D. Suprunenko (1963), *Soluble and Nilpotent Linear Groups*, Translations of Mathematical Monographs, vol. 9, American Mathematical Society, Providence, Rhode Island.

D. A. Suprunenko (1976), *Matrix Groups*, Translations of Mathematical Monographs, vol. 45, American Mathematical Society, Providence, Rhode Island.

Michio Suzuki (1982), *Group Theory I*, Springer-Verlag, New York.

Michio Suzuki (1986), *Group Theory II*, Springer-Verlag, New York.

Tang Shou Wen and Wang Jie (1988), "The primitive permutation groups of degrees 21 to 30", (Chinese), *Beijing Daxue Xuebao* **24**, 269-276.

G. Veronese (1883), "Interprétations géométriques de la théorie des substitutions de $n$ lettres particulièrement pour $n = 3, 4, 5, 6$ en relation avec les groupes de l'hexagramme mystique", *Ann. Mat. Pura Appl.* (2) **11**, 92-236.

William Hulme Wilson (1972), "Primitive irreducible linear groups", MSc thesis, Australian National University.

David L. Winter (1972), "The automorphism group of an extraspecial $p$-group", *Rocky Mountain J. Math.* **2**, 159-168.

Hans J. Zassenhaus (1958), *The Theory of Groups*, 2nd edn, Chelsea Publishing Company, New York.

# Index